Symantec Enterprise Firewall and Symantec Enterprise VPN

Installation Guide for Windows

Supported Platforms
Windows NT
Windows 2000

Part Number: 16-30-00033

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright notice

Copyright © 1998–2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

Portions copyright (c) eHelp Corporation. All rights reserved.

No Warranty

The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. IBM, OS/2, and OS/2 Warp are registered trademarks of International Business Machines Corporation. Novell and NetWare are registered trademarks of Novell Corporation. 3Com and EtherLink are registered trademarks of 3Com Corporation. Compaq is a registered trademark of Compaq Corporation. Zip and Jaz are registered trademarks of Iomega Corporation. SuperDisk is a trademark of Imation Enterprises Corporation, Rainwall is a registered trademark of Rainfinity Corporation. This product includes software developed by the Apache Software Foundation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical support

As part of Symantec Security Response, our global technical support group maintains support centers throughout the world. Our primary role is to respond to specific questions on product feature/function, installation and configuration, as well as author content for our web accessible Knowledge Base. We work collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion, such as working with Product Engineering as well as our Security Research Centers to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Highlights of our offerings include:

- A range of support options giving you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components providing rapid response and up-to-the-minute information
- Software assurance delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures ensure the highest level of protection
- Global support from Symantec Security Response experts is available 24x7 worldwide in a variety of languages
- Advanced features such as the Symantec Alerting Service and Technical Account Manager role offer enhanced response and proactive security support

Please reference our website for current information on Support Programs.

Registration and licensing

If the product you are implementing requires Registration and/or a License Key, the fastest and easiest way to register your service is to access our licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to http://www.symantec.com/techsupp/ent/enterprise.html, select the product you wish to register and, from the Product Home Page select the Licensing and Registration link.

Contacting support

Customers with a current support agreement may contact the Technical Support team via phone or web at www.symantec.com/techsupp.

When contacting support, please be sure to have the following information available

- Product release level
- Hardware information

  Available memory, disk space, NIC information
- Operating system

  Version and patch level
- Network topology

  Router, gateway and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer service

Contact Enterprise Customer Service online at http://www.symantec.com, select the appropriate Global Site for your country, then choose “Service and Support.” Customer Service is available to assist with the following types of issues

- Questions regarding product licensing or serialization
- Update product registration with address or name changes
- General product information (eg. features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advise on Symantec's technical support options
- Non-technical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Copyright notice . . . . . i-ii
Trademarks . . . . . i-ii
Technical support . . . . . i-iii
Highlights of our offerings include: . . . . . i-iii
Registration and licensing . . . . . i-iii
Contacting support . . . . . i-iv
Customer service . . . . . i-iv

Contents

1 Introduction

Intended audience 1-6
Structure 1-6
Related documentation 1-7
New features in V7.0 1-8
High availability/load balancing 1-8
Proxy upgrades 1-8
Improved Symantec Raptor Management Console (SRMC) user interface . . . 1-9
SRMC/Server version exchange 1-9
Remote policies 1-9
Stopping the SEF/SEVPN using SRMC 1-10
AES support 1-10
Read-only firewall support 1-10

2 Developing a security plan

Develop a site security policy 2-12
Define a security plan 2-12
Become security-conscious 2-14
Involve the user community 2-14
Take a pro-active stance 2-15

Worksheets 2-15
Collect information on entities 2-15
Collect information on servers and services 2-16
Define users and user groups 2-18
Choose a method of access 2-19
General access 2-19
VPN access 2-20

3 Pre-installation requirements

Symantec Enterprise Firewall and Symantec Enterprise VPN products 3-22
Cross platform management 3-23
Hardware and software requirements 3-24
Configure your operating system 3-25
Configure network settings 3-27
Windows 2000 network settings 3-27
Windows NT network settings 3-29
Test your network configuration 3-31
Verify the TCP/IP settings 3-31
Test TCP/IP connectivity 3-31
Pre-installation tips 3-34

4 Installing on Windows 2000 and Windows NT

Upgrading previous installations 4-38
Basic upgrade procedures 4-39
Upgrading when the file system will be changed 4-40
Obtaining your license key 4-42
Installation instructions 4-43
Installing SEF or SEVPN and the SRMC 4-43
Installing only the SRMC 4-53
Installing a stand-alone SEF or SEVPN 4-57
Changing your network interface configuration or license 4-65
Connecting to the Symantec Enterprise system 4-67
Uninstalling the SEF/SEVPN products 4-69
Installing RemoteLog 4-69
How Vulture disables unauthorized services 4-70

5 Implementing high availability and load balancing

High availability and load balancing with RainWall 5-71
Installation overviews 5-74
New configurations 5-74
Existing firewall configurations 5-76
Installing RainWall 5-77
Starting and stopping RainWall 5-80
Installing the Symantec Enterprise Firewall 5-80
Modifying rules for use with RainWall 5-81
Uninstalling RainWall 5-81

6 SEF installation verification

Troubleshooting possible problems 6-84
If the installation fails 6-84
Check basic connectivity 6-85
If network connections are unsuccessful 6-88
Installing new network cards 6-88

A Site pre-installation checklist

Security planning A-90
Site hardware information A-92
TCP/IP address A-93
E-mail information for firewall notifications A-94
News service A-95
Special services A-95
Allowed TCP/IP Service A-96
Web service information A-98
Access lists A-99
Entities allowed through the SEF/SEVPN system A-99
Users allowed through the SEF/SEVPN system A-100
Network architecture with a SEF/SEVPN system A-101

Index

Chapter 1

Introduction

This manual describes how to install the Version 7.0 Symantec Enterprise Firewall, Symantec Enterprise VPN, and Symantec Raptor Management Console. Collectively these products are referred to as SEF/SEVPN and SRMC.

This manual describes installation on the following systems:

- Microsoft® Windows®2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows NT®

Consult the *Symantec Enterprise Firewall and Symantec Enterprise VPN Release Notes* for issues related to feature support for the current release or corrections to documentation. Check the Symantec Web site (`www.symantec.com`) for the latest updates to all products.

Intended audience

This manual is intended for system managers or administrators responsible for installing the Symantec Enterprise Firewall or Symantec Enterprise VPN. Installers should have a solid grounding in internetworking concepts and experience installing software on Windows 2000 or Windows NT systems.

Structure

This manual is structured as follows:

Table 1-1 Document structure

Chapter	Title	Content
Chapter 2	Developing a security plan	Lays out basic guidelines for developing an overall security plan. It also explains how to define users and groups and how to configure special services.
Chapter 3	Pre-installation requirements	Contains information on system requirements, networking preliminaries, and license keys.
Chapter 4	Installing on Windows 2000 and Windows NT	Contains instructions for installing the SEF/SEVPN software on Windows 2000 and Windows NT systems.
Chapter 5	Implementing high availability and load balancing	Describes how to use RainWall clusters to create a highly available SEF/SEVPN system with load balancing capabilities.
Chapter 6	SEF installation verification	Verifies your installation has completed properly.
Appendix A	Site pre-installation checklist	Provides a checklist which used to assess your security issues.

Related documentation

The following is a list of documents that provide valuable information concerning Symantec Enterprise Firewall and Symantec Enterprise VPN products and network security procedures:

- *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*, Version 7.0
- *Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide* (PDF file), Version 7.0
- *Symantec Enterprise Firewall and Symantec Enterprise VPN Release Notes*, Version 7.0
- *Symantec Enterprise VPN Client Installation and Configuration Guide*, Version 7.0
- *Symantec Enterprise VPN Client Quick Start Card*, Version 7.0
- *Symantec Enterprise VPN Client Release Notes*, Version 7.0

For the latest information on Symantec network security products, always visit our World Wide Web site at www.symantec.com.

New features in V7.0

The following features are new or enhanced for Symantec Enterprise Firewall and Symantec Enterprise VPN V7.0 for Windows NT or Windows 2000.

High availability/load balancing

Rainfinity's RainWall software provides load balancing and highly available servers, preventing the Symantec Enterprise Firewall or Symantec Enterprise VPN from becoming a single point of failure in a protected network. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for information on configuring RainWall software to work with the SEF/SEVPN.

Note: RainWall is not supported on Windows 2000 systems.

Proxy upgrades

A number of system proxies have been upgraded to make them more robust and to increase the features available to system users. The changed proxies include the following.

SMTP proxy

The SMTP proxy supports ESMTP service extensions from RFC-2681. Security administrators can also add future SMTP service extensions. These extensions are available through the **Services** tab in the **Rules Properties** page.

HTTP proxy

The HTTP proxy supports WebDAV (Web Distributed Authoring and Versioning). WebDAV extensions define a means of searching the Web using title, author, and key words. RFC-2518 defines WebDAV using both HTML and XML for communication between client and server.

RealAudio proxy

The RealAudio proxy supports RealAudio 7.0/8.0 specifications.

H323 proxy

The H323 proxy has been upgraded to support the latest release of Microsoft NetMeeting and T.120 data-sharing connections.

RTSP proxy

The RTSP (Real Time Streaming Protocol) proxy has been added to support real time audio and video from RealPlayer and QuickTime.

Anti-virus scanning

Anti-virus scanning capabilities are now available on HTTP, FTP, and SMTP for firewalls that are connected to a CarrierScan Server.

Improved Symantec Raptor Management Console (SRMC) user interface

The SRMC user interface has been improved to allow simpler management of the SEF/SEVPN system, whether locally or remotely managed. Remote passwords and routes can now be managed using SRMC.

SRMC also supports replication and security policy propagation for managing clustered systems.

SRMC/Server version exchange

The SRMC and the SEF/SEVPN server now exchange version information. Older versions of the SRMC or RMC will not be allowed to connect to 7.0 SEF/SEVPN systems. The V7.0 SRMC, however, can connect to older server versions. Consequently, the new SEF/SEVPN features are supported only on the V7.0 SRMC.

Remote policies

VPN policies (tunnel configuration settings) can now be configured on the SEF/SEVPN system to ease the installation and administration of large numbers of Symantec Enterprise VPN Clients.

Stopping the SEF/SEVPN using SRMC

If you stop the SEF/SEVPN services using the red stop light icon in the SRMC and reboot the host machine, the SEF/SEVPN system preserves its state. In other words, the SEF/SEVPN services remain shut down after the reboot. Traffic cannot pass through SEF/SEVPN when the services are stopped. Consequently, you will need to restart the SEF/SEVPN services after a reboot.

AES support

SEF/SEVPN 7.0 supports the Advanced Encryption Standard (AES), a new cryptographic algorithm used by U. S. government organizations to protect sensitive (unclassified) information. Multiple AES key sizes (128, 192, or 256 bits) provide for increased levels of security.

Read-only firewall support

Version 7.0 of SRMC allows you to set a firewall to read-only mode using `rempass` or the Remote Management Password functionality.

Chapter 2

Developing a security plan

This chapter lays out basic guidelines for developing an overall security plan. It also explains how to define users and groups for the Symantec Enterprise Firewall and Symantec Enterprise VPN and how to configure special services to be passed through these systems.

Develop a site security policy

Before configuring your firewall, it is important to understand exactly what network resources and services you want to protect. It is crucial to have a carefully designed network security policy to guard the valuable resources and information of your organization.

Ideally, your security policy should be captured in a document that describes your organization's network security needs and concerns. Creating this document is the first step in building an effective overall network security system.

To serve your organization well, your policy document must address business as well as security concerns. It should be formulated with, and have support from, top management and anyone responsible for administering security at your site.

The overall success of any policy depends upon the extent to which it balances the perceived inconvenience and cost of security restrictions against the risks and potential cost to the organization of security breaches.

Define a security plan

Your security plan is the detailed implementation of your security policy. Based on the security concerns and trade-offs of your overall policy, your security plan should contain a set of tasks. One of these tasks consists of establishing procedures and rules for access to resources located on your network. These resources include:

- Host computers and servers
- Workstations
- Connection devices (gateways, routers, bridges, and repeaters)
- Terminal servers and remote access servers
- Networking and applications software
- Information in files and databases

SEF/SEVPN is the main tool for enforcing access rules, allowing you to define a set of “Authorization Rules” allowing or denying access to specific resources throughout the network.

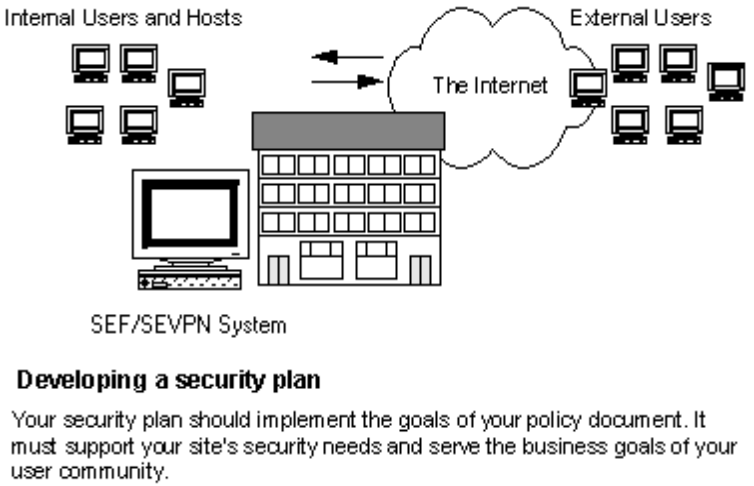

Internal Users and Hosts
External Users
The Internet
SEF/SEVPN System
Developing a security plan
Your security plan should implement the goals of your policy document. It must support your site's security needs and serve the business goals of your user community.

Figure 2-1 Site configuration

Before you begin writing rules to implement your plan using the **Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide**, you should raise and answer at least the following questions:

- How many points of entry exist into your network?

  A firewall defends a single point of entry. Every point of entry should be protected by a firewall.

  A VPN server also defends a single point of entry. You must decide what access the VPN server is going to provide for resources that exist behind the firewall.
- What types of services do you want to allow for internal users?
- To what hosts, subnets, and users do you want to allow these services?
- What external users will you allow to access your network? Which hosts or subnets will you allow them to access? During what hours? For what period of time?
- Do you intend to implement a service network (often called a DMZ)?
- What types of services do you want to allow for external users?
- What type of authentication will you require for external users? (Symantec recommends strong authentication for any access from public networks.)
- If you are implementing VPN tunnels between any internal and external hosts, what types of traffic will be allowed over these tunnels?

- Will you place your web server inside or outside of your protected network?

Become security-conscious

Developing and implementing a security plan for the SEF/SEVPN system you are implementing should be only one part of your overall security policy. SEF/SEVPN offers the best protection against uninvited entry into your network. However, the SEF/SEVPN products cannot guard against entry by people who pirate passwords, any more than a sophisticated lock can stop a thief in possession of the right key.

Take the time to formulate the specific goals of your security plan. Identify the resources you are protecting, and all possible threats. Protecting your resources from unauthorized external users may be only one of your goals. You may also need to limit internal access to certain systems to specific users and groups, within specific time periods.

You should review these issues in detail before you begin configuring the server. Your network's security depends on planning sound policies, implementing them carefully, and checking to see that they work as intended.

Your overall site policy should encompass a number of other factors. Of these, user education is paramount. Publish your company's security policy. Make sure your users are advised of the determination of would-be invaders and the sophistication of available password guessing programs. Make sure they understand how common security breaches are and how costly they can be. These facts alone dictate that users should be encouraged to select passwords that are difficult to crack and to change passwords regularly.

Involve the user community

When developing the details of your security plan, you should solicit the input of group managers or leaders on what services they require, for what users, and so on. Explain to users the need for network security to protect private information, intellectual property, and your business plans.

Before implementing policies, consider notifying the user community of your proposed policies. Doing so in advance can prevent unnecessary frustration on the part of your users.

For instance, if you plan to limit web services to a single server during specific hours, let this be known to the groups and users affected. If you plan to pass all email through a dedicated server, or if external users will be disallowed from accessing certain systems by Telnet, consider passing these changes along before

implementation. Consulting users prior to implementation may save you the time needed to fine-tune those policies later.

Take a pro-active stance

Again, keep in mind that configuring a set of authorization rules on the security gateway is just one piece of your overall security plan. To be effective, this plan should also include:

- Physical security of key systems (especially the security gateway)
- Security risk training for users
- Guidelines on passwords
- Proprietary information policies
- Network planning

Worksheets

To aid you in the planning process, we have provided a set of policy planning worksheets on the pages that follow. Use these worksheets to help implement the specific tasks of your security plan.

After you determine your security plan, additional worksheets to help you implement it are provided in Appendix A.

Collect information on entities

Creating a map like the one shown in **Figure 2-2** is a useful exercise. Doing so requires you to collect and review information on the components that make up the infrastructure of your network.

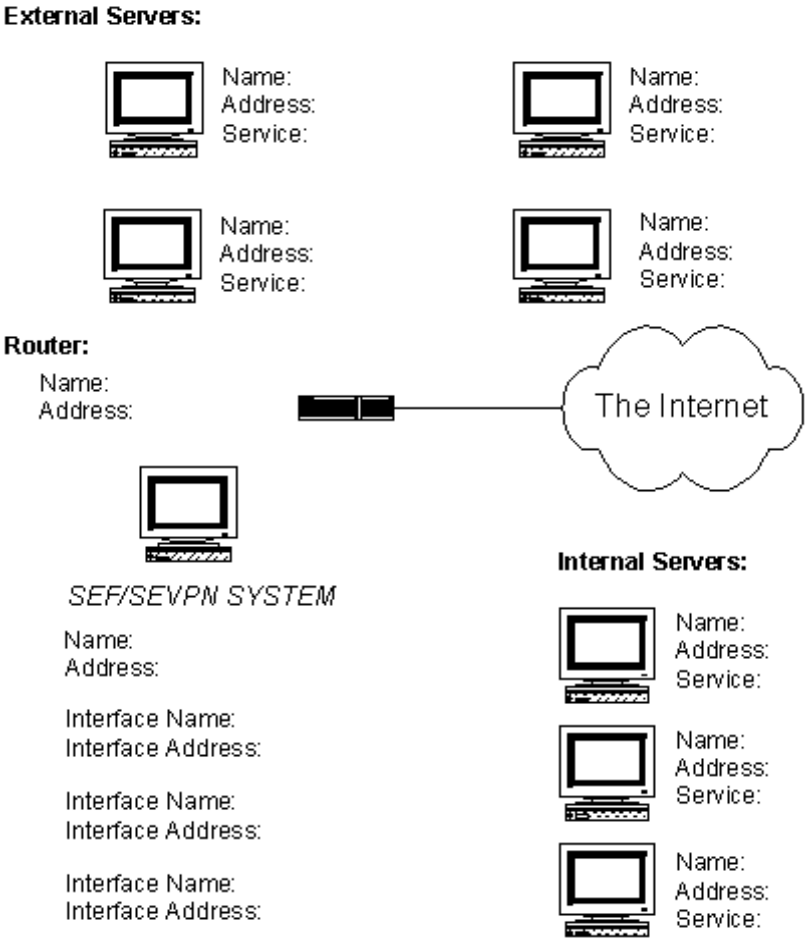


Figure 2-2 Network planning worksheet

Collect information on servers and services

Use the following tables to collect information on the servers and services that make up your security configuration.

Collect information on internal servers

In this table, or a table of your own construction, fill in one line for each of your internal servers that will be accessible from outside the SEF/SEVPN system.

Table 2-1 Internal servers

Internal server name	IP address	Type of service	Port number or range

Collect information on external servers

In this table, fill in one line for each of your external servers that will be accessible from inside the SEF/SEVPN system.

Table 2-2 External servers

External server name	IP address	Type of service	Port number or range

Collect information on service network servers

If you use a service network, in this table, fill in one line for each server on your service network that will be accessible through the SEF/SEVPN system.

Table 2-3 Service network servers

Service network server name	IP address	Type of service	Port number or range

Table 2-3 Service network servers

Service network server name	IP address	Type of service	Port number or range

Collect network information

Collect information and sketch out the main features of your security policy. Your site plan should incorporate policies for DNS (name/IP address resolution), SMTP (firewall email), NNTP (news), FTP (file transfer), HTTP (firewall Web access), and other commonly used services. It should also incorporate policies for any custom protocols or services you plan to pass in or out of your network.

Define users and user groups

After you have sketched out the goals of your security plan, you must enter information on your users in the configuration file database.

The **Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide** explains how to define users and user groups. From the SEF/SEVPN system perspective, your organization consists of a set of *users*. Each user has a unique account ID, and each can exist in a *user group*. Entering information on users and optionally assigning them to functionally related user groups is one of the first tasks in setting up your security framework.

As an example, you may want to create a user group called Accounting, and place in it all accounting personnel.

The idea is to define users and user groups with a view to writing rules and VPN tunnels in support of their goals. The SEF/SEVPN system enables you to fine-tune your user definitions to any level that meets your needs.

Choose a method of access

As you plan your security configuration, you need to decide what methods of access are best for your security needs.

The Symantec Enterprise Firewall provides two ways to connect:

- General access
- VPN access (optional upgrade)

The Symantec Enterprise VPN reverses these two connection alternatives:

- VPN access
- General access (optional upgrade)

For more information about product options, see Table 3-1 on page 23.

General access

General access through the SEF/SEVPN system can be in one of two ways:

- Application proxy with authorization rule
- GSP with authorization rule

When deciding which method is appropriate for a service, use the most secure method that can handle the service. Refer to the **Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide** and the *Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide* for more information.

Application proxy with authorization rule

The Symantec Enterprise Firewall works at the application level and uses a set of application-specific security proxies to evaluate each attempt to pass data in or out of the networks it secures. SEF includes proxies for a variety of common services, including HTTP, secure HTTP, FTP, NNTP, CIFS/SMB, Telnet, SMTP, ping, nbdgram, GOPHER, and RealAudio/Video.

A proxy is a software process that acts as an intermediary between two communications endpoints. A primary task of the proxy is to inspect the application data stream to protect against threats and apply authorization rules that allow or deny selected traffic. Connections using the standard proxies can be authenticated.

GSP with authorization rule

Services not handled by the application proxies included with SEF can be passed by the Generic Service Passer (GSP). For more information, see the **Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide**. Services handled by the GSP are also subject to authorization rules.

The GSP mechanism can handle most types of UDP, TCP, and IP based services.

VPN access

Virtual Private Networking (VPN) uses encryption and encapsulation of packets to provide the security of a private network to information traveling over public networks. It does this by encapsulating each IP packet with additional security information. Any service can be passed and controlled through a VPN tunnel.

There are two types of VPN tunnels:

- Remote client to VPN gateway
- VPN gateway to VPN gateway (site to site)

From a security standpoint, VPN tunnels extend your network. The Symantec Enterprise Firewall and Symantec Enterprise VPN allow you to create filters for these tunnels, which limit the types of connections allowed. The main security feature of a tunnel, however, is that the ends are trusted systems, connected by an encrypted and authenticated path.

A site to site connection involves two Symantec Enterprise VPN systems and the hosts or subnets behind the firewalls.

The Symantec Enterprise Firewall and the Symantec Enterprise VPN use the IPSec/IKE standard, so they can inter-operate with other IPSec/IKE-compliant VPN servers.

For more information on VPN, see the **Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide**.

Chapter 3

Pre-installation requirements

This chapter contains information on pre-installation requirements for the Symantec Enterprise Firewall, Symantec Enterprise VPN, and Symantec Raptor Management Console software, including system and networking requirements, and suggestions for testing network configurations.

Symantec Enterprise Firewall and Symantec Enterprise VPN products

The Symantec Enterprise Firewall and Symantec Enterprise VPN distribution CDs contain several security gateway installation items and combinations of items. (Refer to **Table 3-1 on page 23** for SEF/SEVPN products and their supported features.)

The license key you enter during the installation indicates which SEF/SEVPN products you have purchased. You can purchase licenses for the following:

- Symantec Enterprise Firewall: The Symantec Enterprise Firewall without the VPN capability.
- Symantec Enterprise Firewall and Symantec Enterprise VPN: The Symantec Enterprise Firewall with full VPN capability, via integrated Symantec Enterprise VPN.
- Symantec Enterprise VPN: Provides the proven secure proxying features of the Symantec Enterprise Firewall for users who require VPN capability but do not require a firewall product.
- Symantec Enterprise VPN Client (only with Symantec Enterprise VPN): Formerly RaptorMobile, this product provides safe, transparent, encrypted tunnels from a personal computer to a Symantec Enterprise VPN or a Symantec Enterprise Firewall with VPN. This extends privacy over the unsecured Internet and allows a user to access the private network as if the remote PC were behind the security gateway.

In addition, you can purchase the VelociRaptor, a stand-alone hardware appliance consisting of a box containing logic circuitry, an LCD front panel, and related cabling. The Symantec Enterprise Firewall is preloaded onto VelociRaptor, making the unit ready for use right out of the box.

Table 3-1 Product options

Products		Symantec Enterprise Firewall	Symantec Enterprise Firewall and VPN	Symantec Enterprise VPN	VelociRaptor Firewall Appliance
Options	SRMC	Yes	Yes	Yes	Yes
	Firewall	Yes	Yes	No	Yes
	S2S VPN	No	Yes	Yes	Yes
	Full VPN (SEVPN Client)	No	Yes	Yes	Optional

Note: SRMC is available but optional with the installation of all Symantec Enterprise Firewall and Symantec Enterprise VPN products.

Cross platform management

All Symantec Enterprise Firewall and Symantec Enterprise VPN products support cross platform management through the Symantec Raptor Management Console (SRMC).

- An SRMC installed on Windows NT can manage version 6.5 and 7.0 Symantec Enterprise Firewall (SEF), Symantec Enterprise VPN (SEVPN), and VelociRaptor Firewall Appliance.
- An SRMC installed on Windows 2000 can manage version 6.5 and 7.0 SEF/SEVPN systems, version 6.5 Raptor Firewall and PowerVPN for NT and Solaris, and VelociRaptor Firewall Appliances.

Encryption levels

The SEF/SEVPN media that is available in the United States includes both a 3DES-AES and DES code base.

If you install a 3DES-AES Symantec Enterprise Firewall or Symantec Enterprise VPN, all of the Symantec Raptor Management Consoles (SRMCs) that will be used to manage the security gateway must also be 3DES-AES.

If you install DES Symantec Enterprise Firewall or Symantec Enterprise VPN, all SRMCs that will be used to manage the security gateway must also support DES.

Hardware and software requirements

The system requirements for running version 7.0 of the Symantec Enterprise Firewall or the Symantec Enterprise VPN on a Windows 2000 or Windows NT system are generally the same. They are shown in Table 3-2.

Table 3-2 SEF/SEVPN hardware and software requirements

Component	Requirements	Comments
Hardware		
Network interface cards	A minimum of two network interface cards from the Microsoft Hardware Compatibility List (HCL).	Check the Microsoft web site at www.microsoft.com.
CPU	Intel Pentium III 400 MHz	Multiple processor systems with 2 or more CPU's are supported.
Memory	Sites with less than 200 users: 128 MB, 200-300 MB paging file Sites with more than 200 users: 256 MB, 250-500 MB paging file	More memory is recommended depending on resource usage.
Disk space	Sites with less than 200 users: 2 GB disk with at least 200 MB free space Sites with more than 200 users: 4 GB disk with at least 2 GB free disk space	Symantec Enterprise Firewall and Symantec Enterprise VPN installations requires at least 200 megabytes for configuration and log files.
Software		
Operating systems	Windows NT Windows 2000	Service pack 6a Service pack 2
Browser (for SRMC)	Microsoft Explorer 4.02 or higher	Microsoft Explorer 5.0 is included with Windows 2000.
Management Console	Microsoft Management Console 1.2	The Symantec Raptor Management Console is a plug-in to MMC. The SEF/SEVPN CD contains a file (`immc.exe` in the `ClientSoftware\mmc` directory) that can be used to install MMC 1.2.

The Symantec Enterprise Firewall and Symantec Enterprise VPN do not support RAID level 0 (disk mirroring).

Configure your operating system

Before installing, ensure that your operating system is configured as follows

1 Format your drive as NTFS.

Symantec recommends that the system and partition(s) on which SEF/SEVPN will be installed be formatted using NTFS to take advantage of NTFS file security features.

Note: You must reformat your system to NTFS before obtaining your license key. If you reformat after obtaining your license key, you will need a new key.

---

2 Be sure that all Network Interface Cards (NICs) are installed correctly and have the latest versions of their drivers.

The SEF/SEVPN system requires at least two NICs. All NICs must be connected to different subnets. Each NIC can only have one physical IP address assigned.

Install your network adapters using the TCP/IP protocol only. If you must disable a NIC, remove the driver for that NIC.

Caution: Dynamic Host Configuration Protocol (DHCP) addresses cannot be used by the security gateway. Never configure an adapter in the SEF/SEVPN system to use DHCP to assign any of its IP addresses.

---

3 Install the appropriate service pack:

- Windows 2000 Service Pack 2
- Windows NT Service Pack 6a

These can be found on the Microsoft Web page, http://support.microsoft.com/directory/. Check the *Symantec Enterprise Firewall and Symantec Enterprise VPN Release Notes* and Symantec web site regularly for new service pack recommendations.

4 Check that your sound card is functional.

If you intend to use audio notifications (see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*), you must have a properly installed and configured sound card.

5 If you intend to use pager notifications, you must have a Hayes compatible modem and you must specify its COM port through the Symantec Raptor Management Console window (see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*).

Caution: To maintain security, make sure all modems are configured for dial-out only.

---

6 Install Microsoft Internet Explorer (at least version 4.02).

If you will be running the Symantec Raptor Management Console (SRMC) on Windows NT 4.0, install Microsoft Internet Explorer 4.02 or higher on the NT system. If you will run the SRMC on Windows 2000, there is no need to install IE: it is provided with Windows 2000.

7 Check your routing tables.

- There should only be one default gateway assigned for the system.
- The network adapter or adapters on your internal (inside) network must have no default gateway assigned.
- Configure all (permanent) static routes so that the system can reach all hosts on your inside and outside networks.
- Make sure that a default gateway for the outside interface is assigned.

Configure network settings

The following sections describe the network settings required to run Symantec Enterprise Firewall or the Symantec Enterprise VPN and the processes for configuring them on Windows 2000 and on Windows NT. The same network settings are required to run SEF or the SEVPN.

Note: All unnecessary services, such as NetBEUI, DHCP Server, WINS, and RAS are disabled on all interfaces when the SEF/SEVPN product is installed. Also, NETBIOS and Workstation are disabled on all "outside" or unprotected interfaces.

Windows 2000 network settings

This section describes the processes used to verify Windows 2000 network settings

1. Check that the TCP/IP protocol is installed and bound to all network adapters.
   - From the **Control Panel**, choose **Network and Dial-up Connections**.
   - For each network connection, right click and choose **Properties** to display its **Properties** dialog box.
   - The **Connect Using** field on this dialog box describes the network interface card (NIC) being used to make the connection.
   - Make sure that **Internet Protocol (TCP/IP)** is checked in the components list.
2. Set your computer's Windows 2000 name.

   The spelling of the computer name, the TCP/IP host name, and the host name in the hosts file must match (case does not matter).
   - Click **Start** > **Settings** > **Control Panel** > **System** to display the **System Properties** dialog box.
   - Click the **Network Identification** tab, and then click **Properties** to display the **Identification Changes** dialog box.
   - Use this dialog box to set the computer name. (Windows 2000 computer names are all uppercase.)
   - Click **More** to display the **DNS Suffix and NetBIOS Computer Name** dialog box, and enter the primary DNS suffix of the computer.

For example, if the SEF/SEVPN system's TCP/IP host name is `demo` and `example.net` is the domain name, the fully qualified TCP/IP name is `demo.example.net`.

3 Set your system TCP/IP options.

- Open **Start** > **Settings** > **Control Panel** > **Network and Dial-up Connections**.
- For each network connection, right click and choose **Properties** to display its **Properties** dialog box.
- In the components list, select **Internet Protocol** (**TCP/IP**) and click **Properties.**
- Click Advanced to display the **Advanced TCP/IP Setting** dialog box, and then click the **WINS** tab.
- LMHOSTS lookup is enabled by default. Disable **LMHOSTS lookup**.

4 Verify the IP addresses of your NICs.

- Open **Start** > **Settings** > **Control Panel** > **Network and Dial-up Connections**.
- For each network connection, right click and choose **Properties** to display its **Properties** dialog box.
- In the components list, select **Internet Protocol** (**TCP/IP**) and click **Properties.**
- Use the **Internet Protocol** (**TCP/IP**) **Properties** dialog box to verify the IP address, subnet mask, and default gateway of the NIC.

5 In order for your firewall to be used with DNSd, your resolver must point to the localhost (the loopback address 127.0.0.1). This is entered automatically as the first address in the DNS search order list when the firewall is installed, so it does not require any action on your part prior to installation.

Do not remove the loopback address from the list of DNS server addresses on the **DNS** tab of the **Advanced TCP/IP Settings** page. If the loopback address is accidentally removed, you can use the following procedure to restore it.

- Open the registry with regedit.
- Open the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces` key. Each subkey listed under `Interfaces` is identified by a string of numbers enclosed in brackets.
- Expand each subkey to identify those that correspond to the NICs on the firewall by checking the address value of the key.

- For keys that correspond to NICs on the firewall, add the loopback address to the NameServer value of that key by double-clicking on the NameServer value and entering 127.0.0.1 as the first entry in the list.
- Close the registry editor and reboot the machine.

Windows NT network settings

Use the following process to verify Windows NT network settings

1. Check that the TCP/IP protocol is installed and bound to all network adapters.
   - From the **Network** icon in **Control Panel**, choose the **Protocols** tab and then view the bindings for all protocols.
   - Expand the list under **TCP/IP Protocol** to see which adapters are available and bound to TCP/IP.
2. Set and verify the TCP/IP host name.

   The spelling of the computer name, the TCP/IP host name, and the host name in the hosts file must match (case does not matter).
   - Open **Start** > **Settings** > **Control Panel** > **Networks**.
   - Under Network, click the **Protocols** tab.
   - Highlight **TCP/IP Protocol** and double-click on it.
   - Click the **DNS** tab to set TCP/IP host name and domain name.

     For example, if the SEF/SEVPN system's TCP/IP host name is `demo` and `example.net` is the domain name, the fully qualified TCP/IP name is `demo.example.net`.
3. Set the computer's Windows NT name to match its TCP/IP name.
   - Open **Start** > **Settings** > **Control Panel**.
   - Double-click the **Network** icon and click the **Identification** tab to set the Windows NT name.
   - In the example network, the Windows NT name must be `DEMO` (NT names are all uppercase) because `demo` is the TCP/IP name.

     The Windows NT workgroup or domain name is not related to the TCP/IP domain name. However, if you plan to use Windows NT domain authentication, then the system must be a member of the Windows NT domain which provides authentication.

     See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for instructions for setting up NT domain authentication.

4 Set your system's TCP/IP options.

- Open **Start** > **Settings** > **Control Panel** > **Network**.
- Click the **Protocols** tab.
- Double-click **TCP/IP Protocol**.
- Select the **WINS Address** tab.
- Check the **Enable DNS for Windows Resolution** checkbox.
- Uncheck the **Enable LMHOSTS Lookup** checkbox.

5 Set the DNS search order.

If you want to configure your firewall for use with DNSd, you must point your resolver to the localhost (the loopback address 127.0.0.1).

- Open **Start** > **Settings** > **Control Panel** > **Network**.
- Click the **Protocols** tab.
- Double-click **TCP/IP Protocol**.
- Click the **DNS** tab to set the TCP/IP host name and domain name.
- Enter the IP address of the localhost (127.0.0.1) as the only address in the **DNS Service Search Order** field.

  The DNS configuration may have to be changed during the product installation, depending on how your computer resolves names.

Test your network configuration

Make sure your network is working before you install the Symantec Enterprise Firewall or Symantec Enterprise VPN. After the product is installed, testing network connectivity and tracking down the source of any problems is more complicated.

Verify the TCP/IP settings

Run `ipconfig /all` to verify the IP addresses and netmasks for each network interface.

Test TCP/IP connectivity

You can use `ping` to check whether your network is set up properly. The `ping` command uses Internet Control Message Protocol (ICMP) echo packets to check network connectivity. Run `ping` using the following syntax:

```
ping <IP address>
```

The following example requires SEF/SEVPN systems to allow VPN traffic to flow through the Symantec Enterprise Firewall.

Caution: While you are installing SEF/SEVPN, keep the security gateway disconnected from any public network in order to protect the security of your network.

The following examples use the network configuration displayed in Figure 3-1.

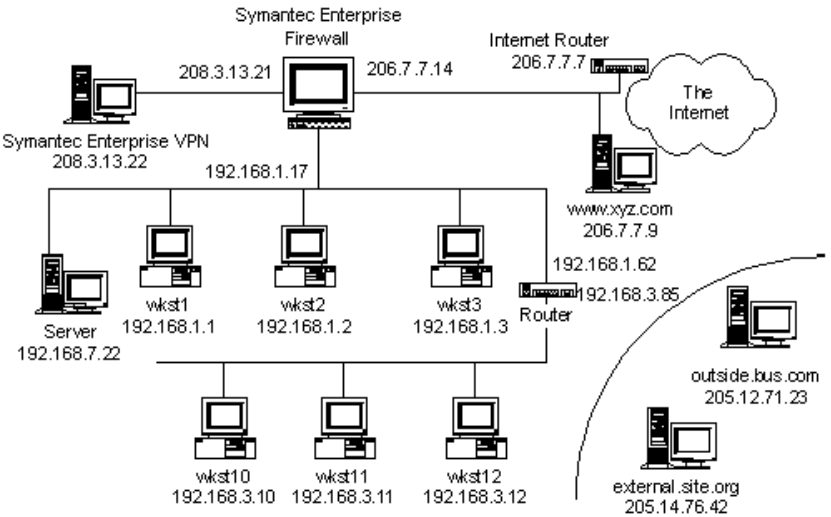


Figure 3-1 Example for testing network connectivity

- From the system on which the product will be installed, `ping` an inside interface IP address.

  ```
  ping 192.168.1.17
  ```

  If this fails:

  - TCP/IP may not be working properly.
  - The network adapter may be misconfigured or defective.

- `Ping` an inside host on the same subnet as the SEF/SEVPN system.

  ```
  ping 192.168.1.1
  ```

  If this fails:

  - The SEF/SEVPN system may not be properly connected to the network. Check that both ends of the cable are connected or try another cable.
  - The network adapter may be defective or misconfigured (configured to use thin net instead of twisted-pair, etc).
  - The system that you are testing with may not be running or connected to the network.

- `Ping` a host on each separate inside non-local subnet.

Before attempting to `ping` an inside subnet, add the static route to demo (the SEF/SEVPN system) using the route command, as in this example:

```
route -p add 192.168.3.0  mask  255.255.255.0
192.168.1.62
```

If this fails:

- The routing information on the system may be incorrect.
- The router may not be configured properly. `ping` the router to verify that it is running.
- The remote system may not be running, connected to the network, or configured properly. Check its default gateway setting. Try to `ping` another host on that subnet.
- The router may be filtering packets. Try to connect via `ftp` or `telnet`. If you receive a *connection refused* or a *connect failed* message within ten seconds, then a connection was probably made (and refused).

• `Ping` the IP address of the SEF/SEVPN system's outside interface.

```
ping 206.7.7.14
```

If this fails:

- TCP/IP may not be properly bound to that network adapter.
- The network adapter may be misconfigured or defective.

• `Ping` a host or router on the local outside network.

```
ping 206.7.7.7
```

If this fails:

- The system may not be properly connected to the network. Check both ends of the cable.
- The network adapter may be defective or misconfigured.
- The system that you are testing with may not be running or connected to the network.

Ping the host

From other systems on the network, `ping` the SEF/SEVPN host. If the SEF/SEVPN system can `ping` a host, that host should be able to `ping` the SEF/SEVPN system.

If there are more than two interfaces in your SEF/SEVPN system, make sure you test each interface by doing the following:

- `ping` the interface by IP address.
- `ping` a host on the same subnet as the interface and on each subnet behind the interface by IP address (inside interface) or `ping` a host on the Internet by IP address (outside interface).

Pre-installation tips

Remember to always log on as a member of the Administrators group

By default, the Vulture process kills any services being run by users other than a member of the Administrators group.

Understand how your network handles name resolution

Whether you maintain the primary DNS server for your domain on-site or your ISP maintains it for you, you must understand and plan the following:

- How your internal systems resolve names of outside and other inside systems.
- How the security gateway resolves inside and outside names.
- How the outside world resolves names for services that your site provides.

If you are using an internal DNS server, make sure that the internal server has both forward and reverse entries for all hosts inside your network so a system can be looked up by its name or its IP address. If you are using the DNS proxy for internal name resolution, enter all systems in the SEF/SEVPN system `hosts` file. If you are using reverse lookups (enabled by default), the system performance can be significantly degraded if it cannot quickly resolve both names and IP addresses of all systems inside and outside of your network.

Understand both the DNS proxy application and dual-level DNS configuration before configuring your system. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* and refer to the *Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide* for details on DNS configuration.

Know which of your addresses need to be published or visible and which need to be hidden from the outside world.

Decide whether your site will be using virtual addresses for any services:

- Virtual addresses may be needed for redirected services. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* and the *Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide* for details.
- Virtual addresses are used if SEF/SEVPN is installed in a RainWall clustering environment. See **Chapter 5, Implementing high availability and load balancing**.

Make arrangements with your Internet service provider in advance

If your network is connected to the Internet, you may need to have new addresses assigned between the router and the security gateway, or your systems on the inside network may need to have new IP addresses assigned (since the security gateways's network adapters must have IP addresses on different subnets).

Services which you were providing to the Internet before installation, such as mail or HTTP, may need to be directed to the outside of the security gateway. If your ISP handles your outside DNS, then they may need to change these entries for you after you complete your installation.

Know which services need to pass through the security gateway

The security gateway provides specialized proxies for the common services (such as HTTP, secure HTTP, FTP, NNTP, SQLNet, Telnet, ping, CIFS/SMB, nbdgram, Gopher, and RealAudio). All of these are listed in the rules-configuration window (see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for details).

The security gateway can pass other services with the Generic Service Passer (see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*). For example, many sites allow inside users to access outside servers using Post Office Protocol version 3 (POP3). GSP can handle this service.

In addition, intermediary proxies such as NTPD and DNSD provide services on the SEF/SEVPN, but do not pass traffic.

Read the release notes

For important information, last minute changes, and known problems, read the *Symantec Enterprise Firewall and Symantec Enterprise VPN Release Notes*.

Note: For access to technical product information, FAQs, and online Symantec Support, visit our Support web site: `www.service.symantec.com`.

If you have purchased a maintenance contract, you must register your software to activate it

1. Go to the **Service and Support** website at `www.service.symantec.com`.
2. Click **I am an Enterprise user.**
3. Select your product and version number and click **Continue**.
4. In the **All Other Services** section, click **Licensing & Registration**.
5. On the **Licensing** page, use the **Register for Support** link to register. The page also provides fax and phone numbers you can use to register the product.

Chapter 4

Installing on Windows 2000 and Windows NT

Once you have completed the preliminaries in **Chapter 3, Pre-installation requirements**, you are ready to install your Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN (SEVPN) product. Installation takes approximately fifteen minutes, provided you have your license key in hand.

Upgrading previous installations

This section describes how to upgrade previous versions of Raptor Firewall or PowerVPN to SEF or SEVPN.

Note: Versions 6.0.2 and 6.5 supported multiple security gateway entities using the same IP address. V7.0 no longer supports this configuration. If you are upgrading from 6.0.2 or 6.5, make sure to eliminate these duplicate entities.

Note: Deny rules with Ratings as a service become invalid after an upgrade. Version 7.0 does not support Ratings as a service in a deny rule. Remove Ratings from deny rules before upgrading to V7.0.

Complete the procedure appropriate to your upgrade situation:

- Follow the **Basic upgrade procedures on page 39** if you are:
  - Upgrading from a version 6.5.2 SEF or SEVPN to version 7.0 of SEF or SEVPN.
  - Upgrading from a version 6.5 Raptor Firewall or PowerVPN to SEF or SEVPN.
  - Upgrading from a version 6.0 Raptor Firewall to SEF or SEVPN. You must obtain a new license before beginning the upgrade procedure.
- Follow the procedure in the section **Upgrading when the file system will be changed on page 40** if the file system on which the Raptor Firewall or PowerVPN was installed will change.

If you are upgrading a Raptor Firewall managed by a remote Raptor Management Console (RMC), keep in mind the following:

- A Symantec Raptor Management Console (SRMC) installed on Windows NT can manage version 6.5.2 and 7.0 SEF/SEVPN systems.
- An SRMC installed on Windows 2000 can manage version 6.5.2 and 7.0 SEF/SEVPN systems and version 6.5 Raptor Firewalls and PowerVPNs for NT and Solaris.
- Managing a version of Raptor Eagle or Eagle Remote prior to 6.0.2 is not supported.

Basic upgrade procedures

If you are upgrading from Raptor Firewall version 6.02 to any version of Symantec Enterprise Firewall or Symantec Enterprise VPN, **you must obtain a new license key** (see **Obtaining your license key on page 42** for instructions).

Uninstalling the previous version

To upgrade from a previous version of Symantec Enterprise Firewall, Symantec Enterprise VPN, Raptor Firewall, or Raptor PowerVPN, you must first uninstall the previous product

---

Caution: Before uninstalling previous versions, you MUST refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Release Notes* for instructions. Not doing so can result in the misconfiguration of your system. Always check the Symantec Web site for the latest version of release notes.

---

1 Before you uninstall, backup your `\raptor\firewall\sg` directory, and the `host` and `host.pub` files.

   Caution: If you are upgrading from a version prior to 6.5.2, you must back up your `pkapps` file before uninstalling. The file must be restored prior to installing version 7.0 of SEF/SEVPN.

   ---

2 Be sure to disconnect the network cable or cables that connect the firewall to any public network.

   Warning: If the computer is hacked in its current state, your firewall configuration information could be copied and used in a later attack.

   ---

3 Uninstall the currently installed product using the procedures in the installation guide and the recommendations in the *Symantec Enterprise Firewall and Symantec VPN Release Notes*.

   The uninstall procedure leaves your configuration files intact on the security gateway. Your new installation will reformat those files.

Upgrading to the new product

Make sure that your system is compatible with the SEF/SEVPN product you want to install and that it has the appropriate software installed. Also, make sure your networking is installed and operating properly, before installing the product.

Follow the instructions in one of the sections under **Installation instructions on page 43** to install your SEF/SEVPN product.

When you first start the 7.0 SRMC, you MUST select **Save All** from the **Action** > **All Tasks** menu to save your new 7.0 configuration file formats.

Caution: Upon starting the 7.0 SRMC, if you have invalid configurations, performing a Save All will automatically delete these invalid configurations. In this case, you should attempt to correct these configuration issues before selecting **Save All** so that data is not deleted.

All 6.0.x configuration files with formats that have changed in 7.0 are kept intact and are backed up into a directory named `60Files` in the `Raptor\Firewall\sg` directory.

Note: When you upgrade from a version 6.0 RMC to a version 7.0 SRMC, only the localhost (if present) appears in your 7.0 snap-in. SRMC V7.0 assumes any other systems you have remotely managed from this SRMC are still V6.0.x. SRMC does not automatically upgrade host connections for remotely managed systems. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for instructions on upgrading host connections.

Upgrading when the file system will be changed

This procedure describes how to save your previous configuration if your upgrade procedure involves changing the file system (usually from FAT to NTFS) and therefore the Volume ID of the partition where the security gateway will be installed.

Caution: You must perform the following procedure in the order in which it is written. If you install the Symantec Enterprise Firewall or Symantec Enterprise VPN before restoring the original configuration using `skstool`, your data will be corrupted.

Be sure to disconnect the network cable or cables that connect the security gateway to any public network.

Warning: If the computer is hacked in its current state, your security gateway configuration information could be copied and used in a later attack.

Complete the following steps to save your configuration using `skstool`

1. Insert the Symantec Enterprise Firewall or Symantec Enterprise VPN CD-ROM and copy the file `skstool.exe` from the `\symc_fw_vpn\upgrade\3DES` or `DES` directory to your system.

   The directory you copy from depends on the encryption standard used for the previous product installation.

2. From a DOS prompt, access the directory to which you copied `skstool.exe` and enter the following command:

   ```
   skstool
   ```

3. Enter and confirm a recovery password. Store this password for use when you have upgraded your operating system and are ready to recover the configuration files.

4. Copy the `host` and `host.pub` files from `\System32\drivers\etc` and the configuration files located in the `\Raptor\firewall\sg` directory to a backup location. In most cases, these files will fit on a floppy disk.

5. Uninstall your existing product.

6. Upgrade the operating system.

7. Determine the Volume ID of the partition where you plan to install the SEF/SEVPN product by typing `vol` at the DOS prompt.

8. Obtain a new license key by following the instructions in **Obtaining your license key on page 42**.

9. Restore your security gateway configuration by completing the following steps:

   a. From a DOS prompt, access the directory to which you copied `skstool.exe` and enter the following command:

      ```
      skstool
      ```

   b. Enter the recovery password you set on the original host to restore your secret keys on the new host.

10. Install your SEF/SEVPN product by following the instructions in one of the sections under **Installation instructions on page 43**.

Note: This procedure assumes that the new configuration has the same IP addresses and hostname as the original. If it does not, you must edit configuration files by hand after the procedure is completed.

Obtaining your license key

A new license key is required if you are performing a new installation or upgrading from version 6.0 or earlier of Raptor Firewall or Raptor PowerVPN.

To obtain your license key

1. Open a command prompt window on the machine where you will install the SEF/SEVPN product.
2. Type the following command:

```
C:\>vol %systemdrive%
     Volume in drive C has no label.
     Volume Serial Number is nnXn-nnnX
```

3. Record the Volume Serial Number for use in applying for your license.
4. To use the online license key generator:
   a. Go to the **Service and Support** page of the Symantec website at `http://www.symantec.com/techsupp`.
   b. Check **I am an enterprise user**.
   c. Select your product and version number and click **Continue**.
   d. Scroll down the page to the **All Other Services** section and click **Licensing & Registration**.
   e. Follow the instructions on the **Licensing** page to obtain your license.

Remember that each product requires a different key. A Symantec Enterprise Firewall key will not work for Symantec Enterprise VPN, for instance.

Once you have your license key, install the product according to instructions in this chapter.

You can install without a license key for a 30 day evaluation copy. To add a license key later, run the installation process, as described in the following section.

Installation instructions

There are multiple ways to install the Symantec security gateway products

- Install the Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN (SEVPN) and the Symantec Raptor Management Console (SRMC)
- Install SEF or SEVPN as a stand-alone system without the SRMC
- Install the SRMC alone, to be used to manage remote systems

Installing SEF or SEVPN and the SRMC

To install SEF or SEVPN and the Symantec Raptor Management Console (SRMC)

1. Log in as the Local Administrator or as a user in the Local Admin group.
2. Insert the Symantec Enterprise Firewall or Symantec Enterprise VPN distribution CD.
3. Browse to one of the following directories.

   `SYMC_fw_vpn\3DES`(High Encryption)
   `SYMC_fw_vpn\DES`
4. Double click the file `setup.exe` to launch the installation and display the **Welcome to Setup** window.

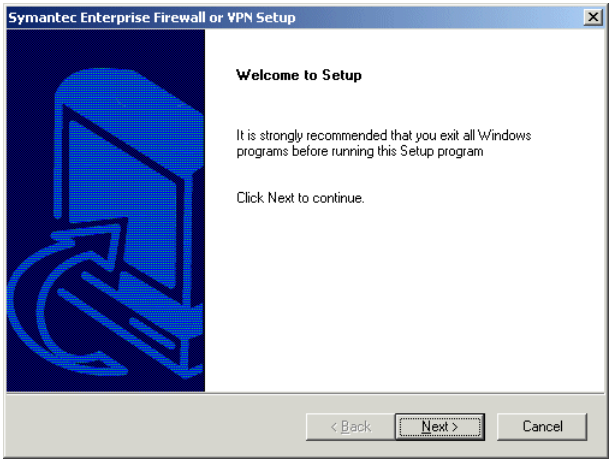

Symantec Enterprise Firewall or VPN Setup
Welcome to Setup
It is strongly recommended that you exit all Windows programs before running this Setup program
Click Next to continue.
< Back
Next >
Cancel

Figure 4-1 Welcome to Setup window

5 Click **Next** to display the **License Agreement**.

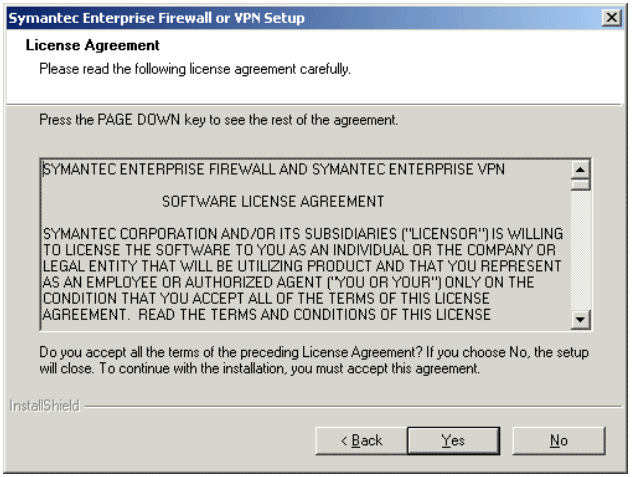

Symantec Enterprise Firewall or VPN Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
SYMANTEC ENTERPRISE FIREWALL AND SYMANTEC ENTERPRISE VPN
SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To continue with the installation, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 4-2 SEF/SEVPN setup: License Agreement

6 Read the License Agreement, and then click **Yes** to accept the agreement and display the **Product License Key** screen.

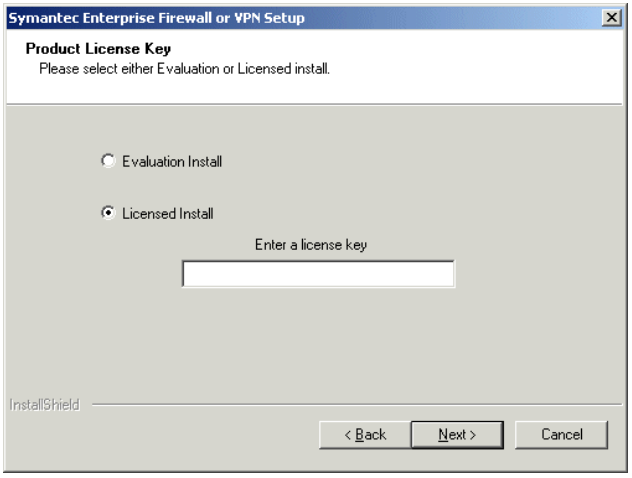


Figure 4-3 SEF/SEVPN setup: Product License Key

Note: You must obtain a new license key if you are upgrading from version 6.0 or earlier.

7 Do one of the following:

- If you have a license for the SEF/SEVPN product you want to install, click **Licensed Install** and enter the license key in the field provided. Remember that the key is upper-case. Then click **Next**.
- If you want to install a 30-day evaluation copy, click **Evaluation Install** and then click **Next**. The install procedure does a preliminary validation of the key and displays the **Product Selection** screen.

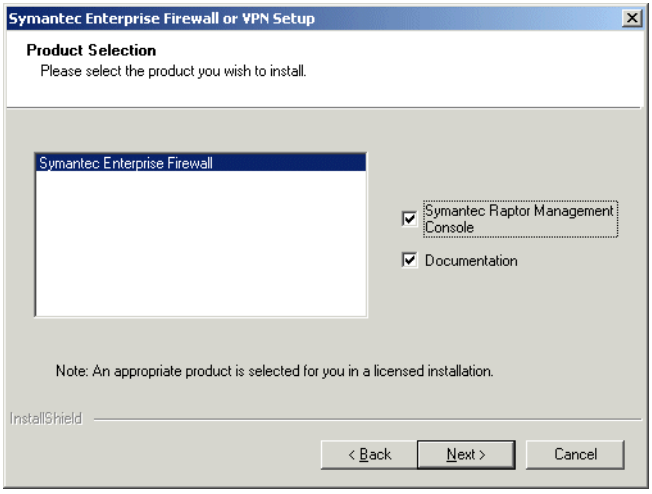

Symantec Enterprise Firewall or VPN Setup
Product Selection
Please select the product you wish to install.
Symantec Enterprise Firewall
Symantec Raptor Management Console
Documentation
Note: An appropriate product is selected for you in a licensed installation.
InstallShield
< Back
Next >
Cancel

Figure 4-4 SEF/SEVPN setup: Product Selection

If you entered a license key, the **Product Selection** screen displays the product that is valid for your license key, as shown in Figure 4-4. The possibilities are:

Symantec Enterprise Firewall
Symantec Enterprise Firewall with Symantec Enterprise VPN
Symantec Enterprise VPN

If you selected Evaluation Install, all the installation options above are available. Choose the product to install.

8 Check **Symantec Raptor Management Console**.

9 If you want to install PDF files for the Symantec Enterprise Firewall and Symantec Enterprise VPN documentation, check **Documentation**.

10 Click **Next** to display the **Destination Drive** screen.

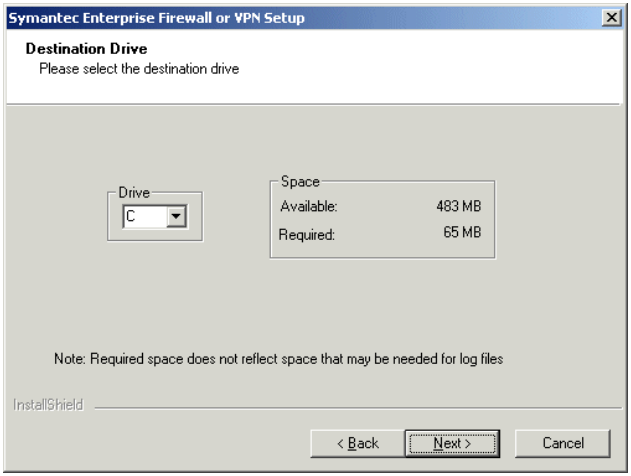


Figure 4-5 SEF/SEVPN setup: Destination Drive

11 Choose a drive to which to install the SEF/SEVPN files. The **Space** listing changes to reflect the available space on the drive you choose.

12 Click **Next** to display the **Install Selected Components** screen, which contains a summary of your installation selections.

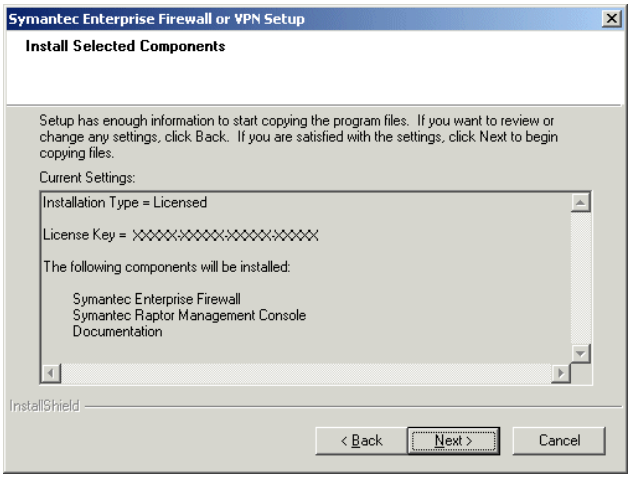

Symantec Enterprise Firewall or VPN Setup
Install Selected Components
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Installation Type = Licensed
License Key = XXXXX-XXXXX-XXXXX-XXXXX
The following components will be installed:
Symantec Enterprise Firewall
Symantec Raptor Management Console
Documentation
InstallShield
< Back
Next >
Cancel

Figure 4-6 SEF/SEVPN setup: Install Selected Components

13 Review your choices, then click **Next**. The SRMC installation displays the **Symantec Raptor Management Console Setup Welcome** screen.

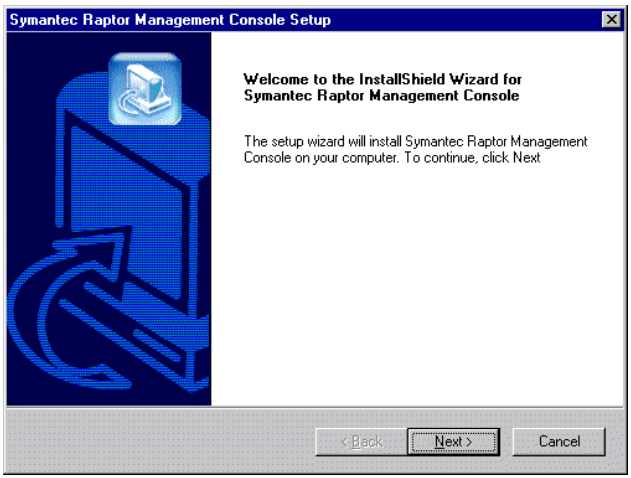

Symantec Raptor Management Console Setup
Welcome to the InstallShield Wizard for Symantec Raptor Management Console
The setup wizard will install Symantec Raptor Management Console on your computer. To continue, click Next
< Back
Next >
Cancel

Figure 4-7 Symantec Raptor Management Console Setup Welcome

14 Click **Next** to display the **SRMC License Agreement** screen.

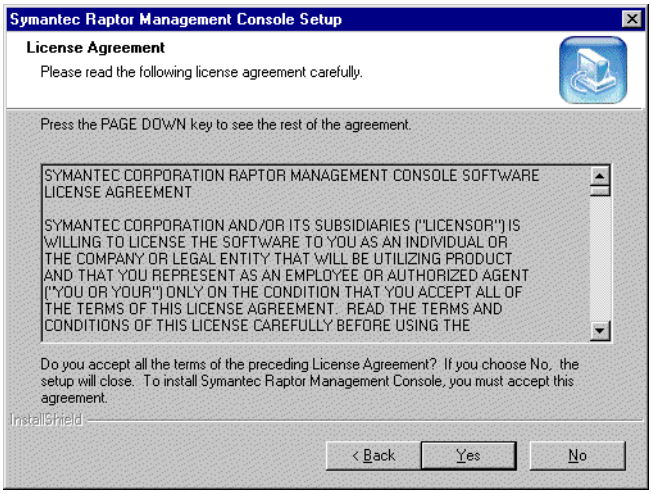

Symantec Raptor Management Console Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
SYMANTEC CORPORATION RAPTOR MANAGEMENT CONSOLE SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Symantec Raptor Management Console, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 4-8 SRMC setup: License Agreement

15 Read the License Agreement, then click **Yes** to display the **Choose Destination Location** screen.

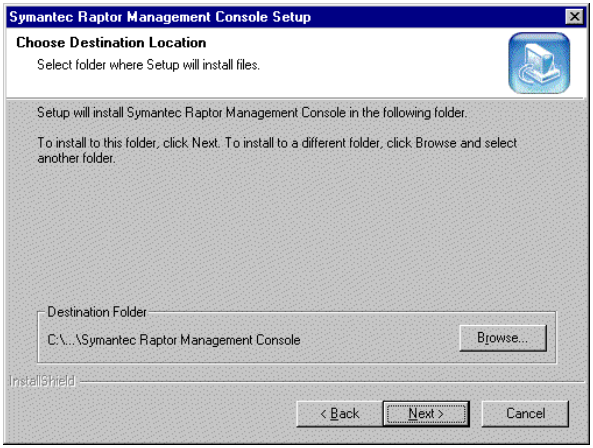

Symantec Raptor Management Console Setup
Choose Destination Location
Select folder where Setup will install files.
Setup will install Symantec Raptor Management Console in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\Symantec Raptor Management Console
Browse...
InstallShield
< Back
Next >
Cancel

Figure 4-9 SRMC setup: Choose Destination Location

16 Do one of the following:

- Accept the default location, which is `C:\Program Files\Symantec\Symantec Raptor Management Console`, for the installation of the SRMC files.
- Use the **Browse** button to specify an alternative location.

17 Click **Next**. The **Start Copying Files** screen indicates your installation choices.

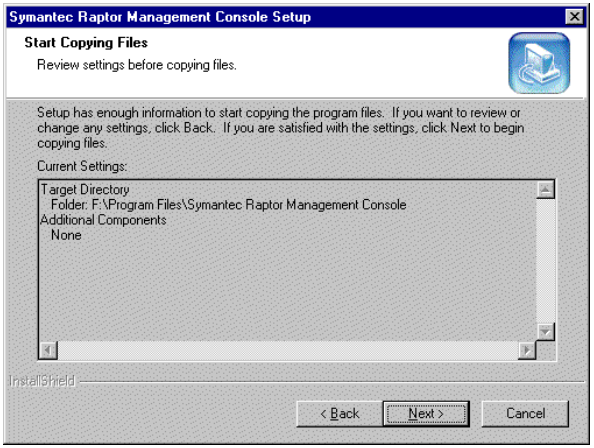

Symantec Raptor Management Console Setup
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Target Directory
Folder: F:\Program Files\Symantec Raptor Management Console
Additional Components
None
InstallShield
< Back
Next >
Cancel

Figure 4-10 SRMC setup: Start Copying Files

18 Review your choices, then click **Next** to start the installation of the SRMC files. The **Symantec Raptor Management Console Setup Status** screen indicates the progress of the installation.

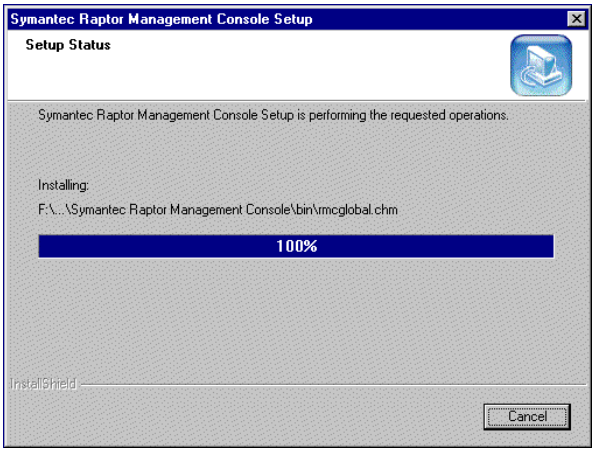


Figure 4-11 SRMC setup: Setup Status

When the SRMC is completely installed, the SEF/SEVPN **Setup Status** screen is displayed, showing the progress of the security gateway installation.

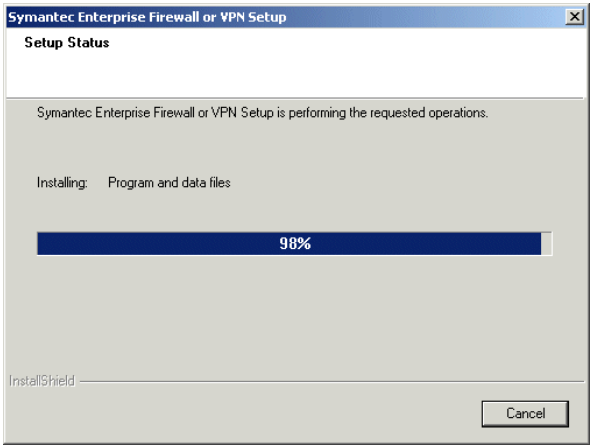


Figure 4-12 SEF/SEVPN setup: Setup Status

If you are installing on Windows NT, additional screen messages tell you that non-essential services are stopped, and restarted. When all the files have been

copied, the **Symantec Enterprise Firewall or VPN Configuration** dialog box is displayed.

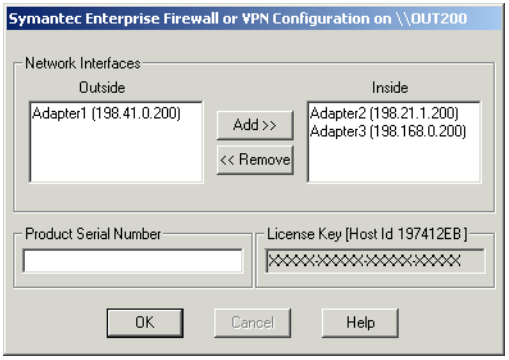


Figure 4-13 Symantec Enterprise Firewall or VPN Configuration

19 Select a network interface or interfaces to be the Inside interface and use the **Add** >> button to move it to the **Inside** box. A screen message reminds you that the inside interface cannot have a default gateway set. See **Configure network settings on page 27**.

20 Click **OK** to close the Symantec Enterprise Firewall or VPN Configuration dialog box. The **Local Management Password** dialog box is displayed.

Note: Clicking **Cancel** at this point closes this window. It does not cancel the installation. If you want to cancel at this time, finish the installation and then uninstall with the **Uninstall** menu item.

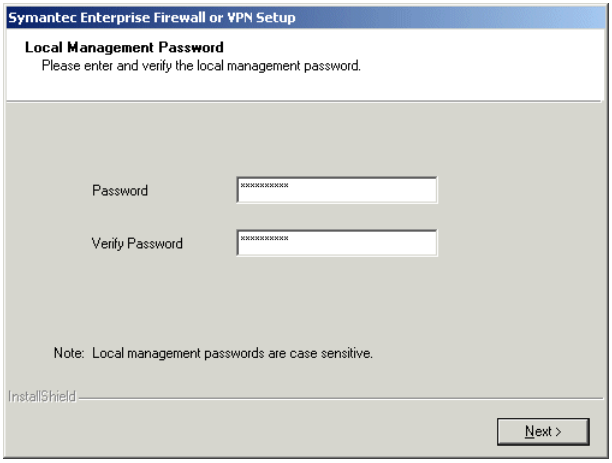


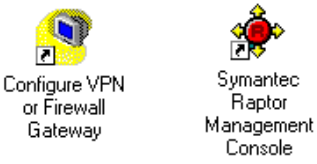
Figure 4-14 SEF/SEVPN setup: Local Management Password

21 Enter and confirm a local management password. You must enter this password to manage any SEF/SEVPN product locally. Note that passwords are case-sensitive.

22 Click **Next** to process the local management password and complete the installation of the Symantec Enterprise Firewall or Symantec Enterprise VPN.

23 Restart your computer when prompted.

The installation process adds two shortcut icons to your desktop:



- The **Configure VPN or Firewall Gateway** icon allows you to configure the security gateway as described in Changing your network interface configuration or license on page 65.
- The **Symantec Raptor Management Console** icon allows you to run the SRMC as described in Connecting to the Symantec Enterprise system on page 67.

A **Symantec Enterprise Firewall or VPN** item is added to the **Programs** group of your **Start** button menu. It contains the following options:

- Configure VPN or Firewall Gateway
- Uninstall VPN or Firewall Gateway

If you also installed the SRMC, a **Symantec Raptor Management Console** item is added to the **Programs** group, containing the following options:

- Raptor Management Console
- Uninstall Raptor Management Console

Installing only the SRMC

The following procedure describes how to install the SRMC without installing the Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN (SEVPN). This allows you to install on a separate Microsoft Windows 2000 Professional or Server, or Microsoft Windows NT Server and use the SRMC to manage firewall systems remotely.

If you want to install the SRMC on the same machine on which you install the Symantec Enterprise Firewall or Symantec Enterprise VPN, see **Installing SEF or SEVPN and the SRMC on page 43**.

Note: Installation of the SRMC does NOT require a license key.

---

1. Insert the Symantec Enterprise Firewall or Symantec Enterprise VPN distribution CD-ROM.
2. Browse to one of the following directories:

   `ClientSoftware\SymantecRMC\3DES` (High Encryption)
   `ClientSoftware\SymantecRMC\DES`
3. Double-click the file `setup.exe`. to begin the installation and display the **Symantec Raptor Management Console Setup Welcome** screen.

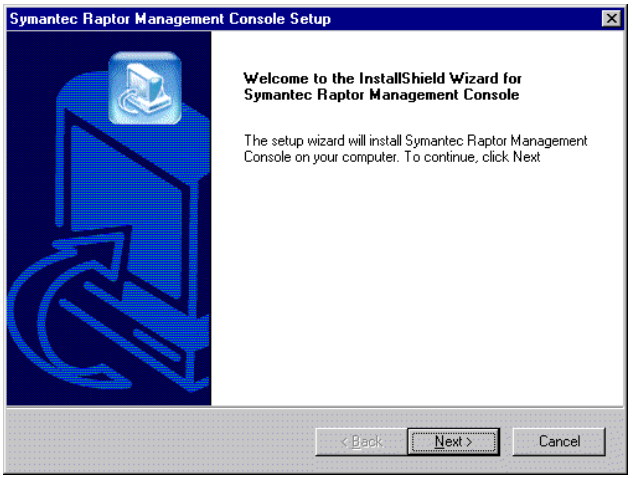

Symantec Raptor Management Console Setup
Welcome to the InstallShield Wizard for Symantec Raptor Management Console
The setup wizard will install Symantec Raptor Management Console on your computer. To continue, click Next
< Back
Next >
Cancel

Figure 4-15 Symantec Raptor Management Console Setup Welcome

4 Click **Next** to display the **License Agreement**.

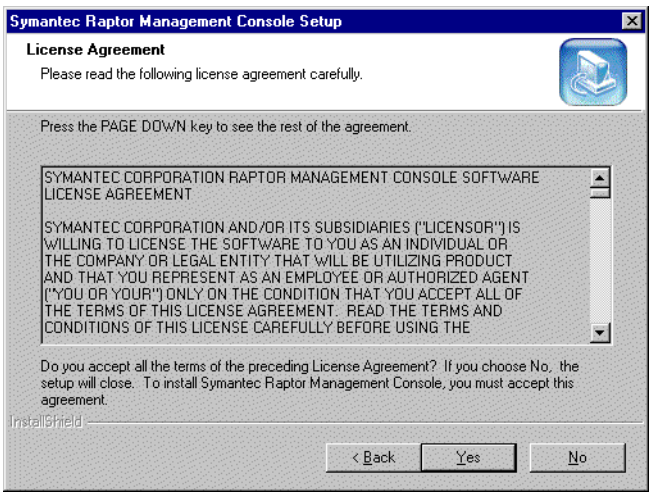

Symantec Raptor Management Console Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
SYMANTEC CORPORATION RAPTOR MANAGEMENT CONSOLE SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Symantec Raptor Management Console, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 4-16 SRMC setup: License Agreement

5 Read the License Agreement, then click **Yes** to display the **Choose Destination Location** screen.

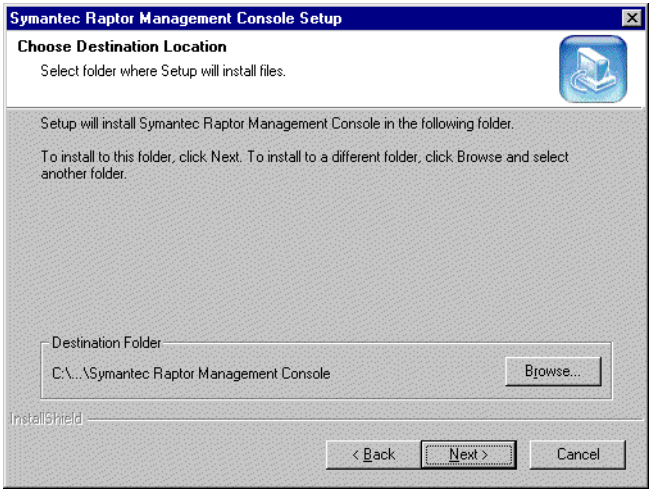

Symantec Raptor Management Console Setup
Choose Destination Location
Select folder where Setup will install files.
Setup will install Symantec Raptor Management Console in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\Symantec Raptor Management Console
Browse...
InstallShield
< Back
Next >
Cancel

Figure 4-17 SRMC setup: Choose Destination Location

6 Accept the default location (`C:\Program Files\Symantec\Symantec Raptor Management Console`) for the installation of the SRMC files or use the **Browse** button to specify an alternative location.

7 Click **Next** to display the **Start Copying Files** screen, showing your installation choices.

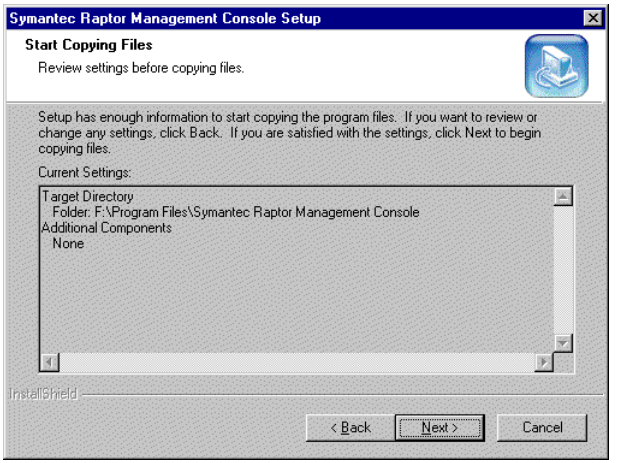

Symantec Raptor Management Console Setup
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Target Directory
Folder: F:\Program Files\Symantec Raptor Management Console
Additional Components
None
InstallShield
< Back
Next >
Cancel

Figure 4-18 SRMC setup: Start Copying Files

8 Review your choices, then click **Next** to start the installation of the Symantec Raptor Management Console. The **Symantec Raptor Management Console Setup Status** screen indicates the progress of the installation.

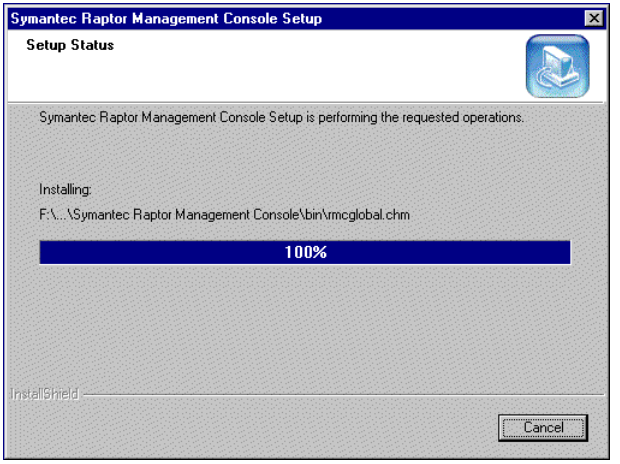


Figure 4-19 SRMC setup: Setup Status

When all files are installed, the **InstallShield Wizard Complete** screen is displayed.

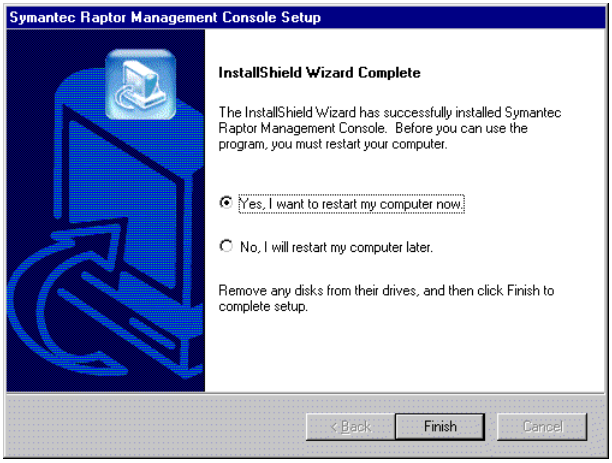

Symantec Raptor Management Console Setup
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Symantec Raptor Management Console. Before you can use the program, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

Figure 4-20 SRMC setup: InstallShield Wizard Complete

9 Click **Finish** to complete the installation and restart your computer.

The installation procedure adds the **Symantec Raptor Management Console** icon to your desktop. Use this icon to display the SRMC as described in **Connecting to the Symantec Enterprise system on page 67**.

A Symantec Raptor Management Console item is added to the **Programs** group of your **Start** menu. It contains the following items.

- Symantec Raptor Management Console
- Uninstall Symantec Raptor Management Console

Installing a stand-alone SEF or SEVPN

The following installation procedure is used to install a stand-alone version of the Symantec Enterprise Firewall or Symantec Enterprise VPN, without installing the Symantec Raptor Management Console (SRMC). The SEF/SEVPN product you install can be managed remotely by an SRMC installed on another system.

1 Log in as the Local Administrator or as a user in the Local Admin group.

2 Insert the Symantec Enterprise Firewall or Symantec Enterprise VPN distribution CD.

3 Browse to one of the following directories.

`SYMC_fw_vpn\3DES`(High Encryption)
`SYMC_fw_vpn\DES`

4 Double click the file `setup.exe` to start the installation and display the **Symantec Enterprise Firewall or VPN Setup Welcome** screen.

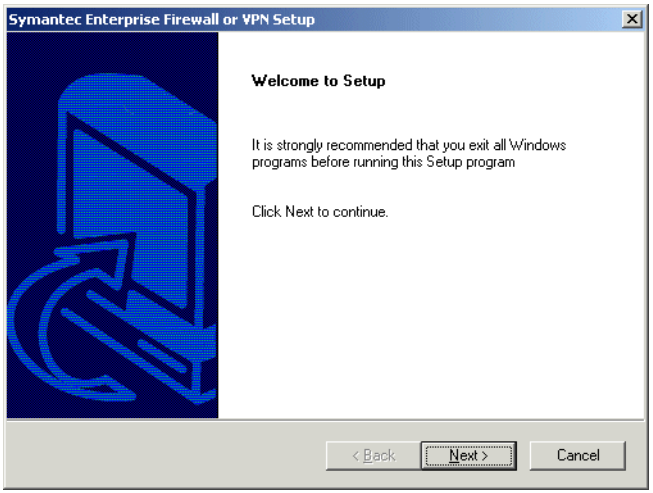

Symantec Enterprise Firewall or VPN Setup
Welcome to Setup
It is strongly recommended that you exit all Windows programs before running this Setup program
Click Next to continue.
< Back
Next >
Cancel

Figure 4-21 SEF/SEVPN setup: Welcome

5 Click **Next** to display the **License Agreement**.

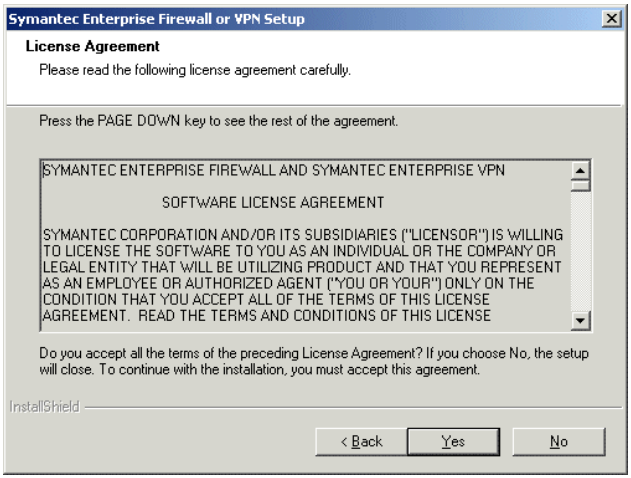

Symantec Enterprise Firewall or VPN Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
SYMANTEC ENTERPRISE FIREWALL AND SYMANTEC ENTERPRISE VPN
SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To continue with the installation, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 4-22 SEF/SEVPN setup: License Agreement

6 Read the License Agreement, and then click **YES** to accept the agreement and display the **Product License Key** screen.

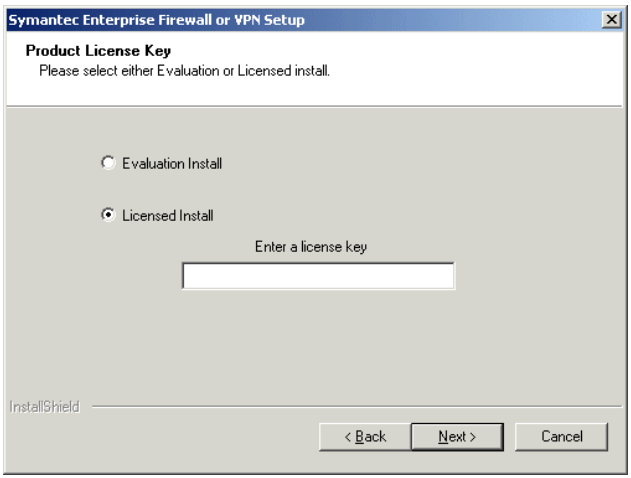


Figure 4-23 SEF/SEVPN setup: Product License Key

Note: You must obtain a new license key if you are upgrading from version 6.0 or earlier.

7 Do one of the following:

- If you have a license for the SEF/SEVPN product you want to install, click **Licensed Install** and enter the license key in the field provided. Remember that the key is case sensitive. Then click **Next**.
- If you want to install a 30-day evaluation copy, click **Evaluation Install** and then click **Next**.

The install procedure does a preliminary validation of the key and displays the **Product Selection** screen.

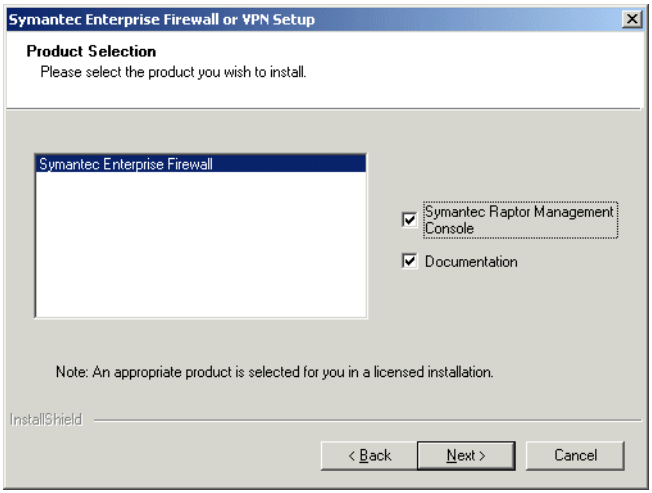

Symantec Enterprise Firewall or VPN Setup
Product Selection
Please select the product you wish to install.
Symantec Enterprise Firewall
Symantec Raptor Management Console
Documentation
Note: An appropriate product is selected for you in a licensed installation.
InstallShield
< Back
Next >
Cancel

Figure 4-24 SEF/SEVPN setup: Product Selection

If you entered a license key, the Component Installation screen displays the product that is valid for your license key, as shown in Figure 4-24. The possibilities are:

Symantec Enterprise Firewall
Symantec Enterprise Firewall with Symantec VPN
Symantec Enterprise VPN

If you selected Evaluation Install, all the installation options above are available. Choose the product to install.

8 Leave **Symantec Raptor Management Console** unchecked.

9 If you want to install PDF files for the Symantec Enterprise Firewall and Symantec Enterprise VPN documentation, check **Documentation**.

10 Click **Next** to display the **Destination Drive** screen.

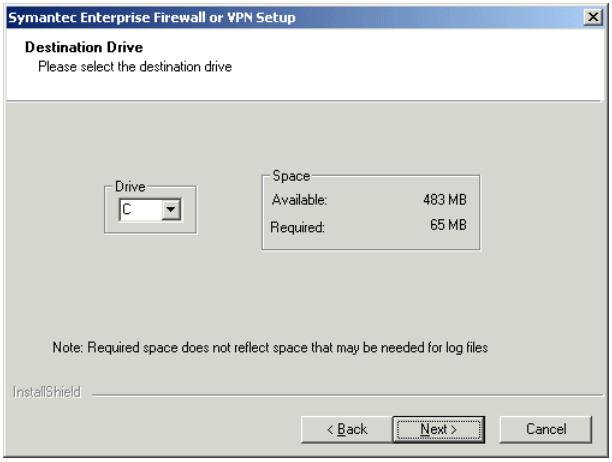


Figure 4-25 SEF/SEVPN setup: Destination Drive

11 Choose a drive to which to install the SEF/SEVPN files. The **Space** listing changes to reflect the available space on the drive you choose.

12 Click **Next** to display the **Install Selected Components** screen, which contains a summary of your installation selections.

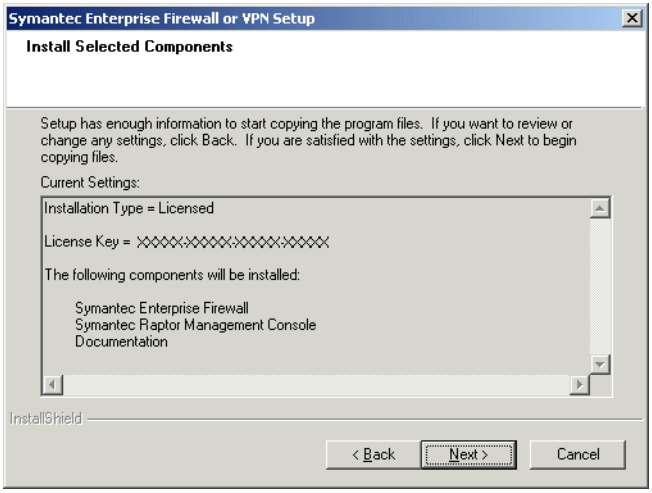

Symantec Enterprise Firewall or VPN Setup
Install Selected Components
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Installation Type = Licensed
License Key = XXXXX-XXXXX-XXXXX-XXXXX
The following components will be installed:
Symantec Enterprise Firewall
Symantec Raptor Management Console
Documentation
InstallShield
< Back
Next >
Cancel

Figure 4-26 SEF/SEVPN setup: Install Selected Components

13 Review your choices, then click **Next**. The **Setup Status** screen shows the progress of the installation.

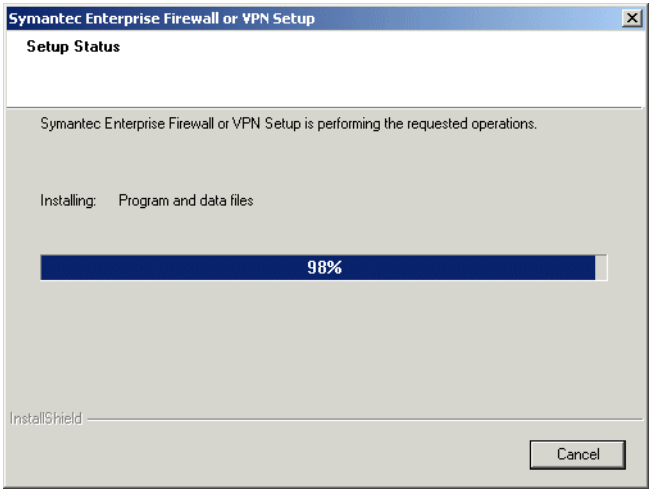


Figure 4-27 SEF/SEVPN setup: Setup Status

If you are installing on Windows NT, additional screen messages tell you that non-essential services are stopped, and restarted. When all the files have been

copied, the **Symantec Enterprise Firewall or VPN Configuration** dialog box is displayed.

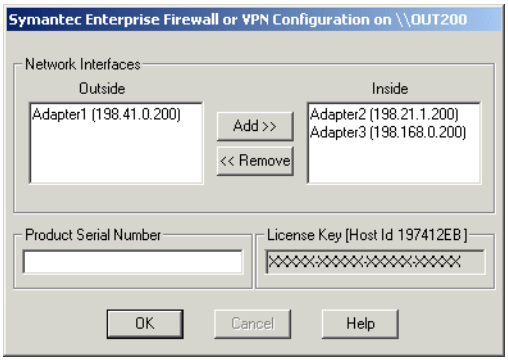


Figure 4-28 Symantec Enterprise Firewall or VPN Configuration

14 Select a network interface or interfaces to be the Inside interface and use the **Add** >> button to move them to the **Inside** box. A screen message reminds you that the inside interface cannot have a default gateway set. See **Configure network settings on page 27**.

15 Click **OK** to close the **Symantec Enterprise Firewall or VPN Configuration** dialog box. The **Local Management Password** dialog box is displayed.

Note: Clicking **Cancel** at this point closes this window. It does not cancel the installation. If you want to cancel at this time, finish the installation and then uninstall with the **Uninstall** menu item.

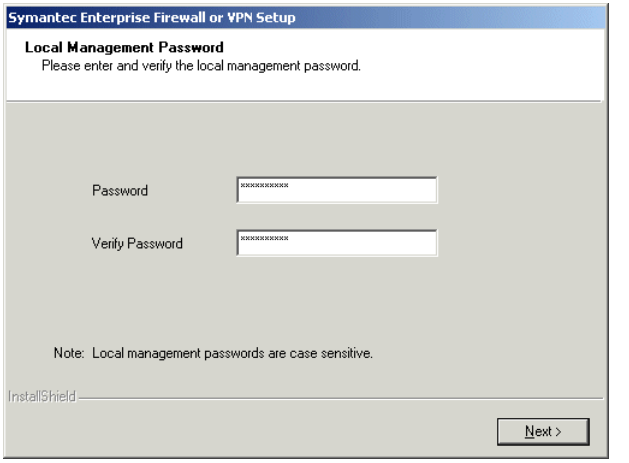


Figure 4-29 SEF/SEVPN setup: Local Management Password

16 Enter and confirm a local management password. You must enter this password to manage any SEF/SEVPN product locally. Note that passwords are case-sensitive.

17 Click **Next** to process the local management password and complete the installation of the Symantec Enterprise Firewall or Symantec Enterprise VPN.

18 Restart your computer when prompted.

A **Symantec Enterprise Firewall or VPN** item is added to the **Programs** group of your **Start** button menu. It contains the following options:

- Configure VPN or Firewall Gateway
- Uninstall VPN or Firewall Gateway:

Changing your network interface configuration or license

The **Symantec Enterprise Firewall or VPN Configuration** utility, which is installed when you install SEF or SEVPN, can be used to:

- Change the configuration of your network interfaces
- Change your license (for example, if you want to upgrade from an evaluation installation to a fully licensed installation)

Caution: Before you make a change to your SEF or SEVPN configuration, you should notify your users. Changing the network interface configuration requires a reboot of the firewall server. Changing your license information momentarily stops the firewall service.

To change your network interface configuration

1 Double-click on the **Configure VPN or Firewall Gateway** icon on your desktop.

or

Click **Start** > **Programs** > **Symantec Enterprise Firewall or VPN** > **Configure VPN or Firewall Gateway**.

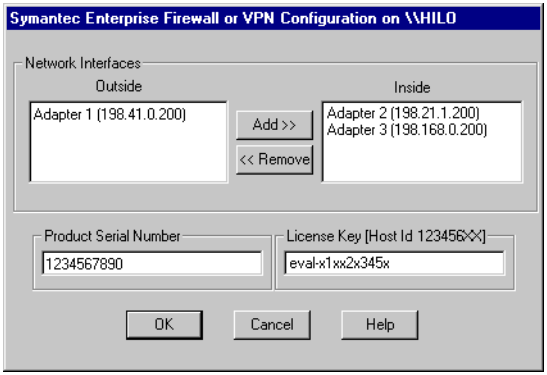


Figure 4-30 Symantec Enterprise Firewall or VPN Configuration

2 To specify a network interface as an inside interface, select it in the **Outside** list, then click the **Add** >> button. It is moved to the **Inside** list.

3 To specify a network interface as an outside interface, select it in the **Inside** list and click the << **Remove** button. It is moved to the **Outside** list.

Note: This does not remove the interface from the list but designates it as outside.

---

4 Click **OK**.

5 Reboot your system when prompted.

To change your license

1 Obtain a license as described in **Obtaining your license key on page 42**.

2 Display the **Symantec Enterprise Firewall or VPN Configuration** dialog box as described in the previous procedure.

3 Enter your new license key in the **License Key** field.

4 Click **OK**. The SEF or SEVPN service is momentarily stopped and then restarted.

Connecting to the Symantec Enterprise system

To connect to a Symantec Enterprise Firewall or Symantec Enterprise VPN

1 Click on the **Symantec Raptor Management Console** icon on your desktop.

or

Click **Start** > **Symantec Raptor Management Console** > **Raptor Management Console**.

The Symantec Raptor Management Console is opened on your desktop.

2 In the left pane, click the **Symantec Raptor Management Console** icon in the root directory (below the Symantec Raptor Management icon), as shown in Figure 4-31. This displays the **Getting Connected** taskpad in the right pane.

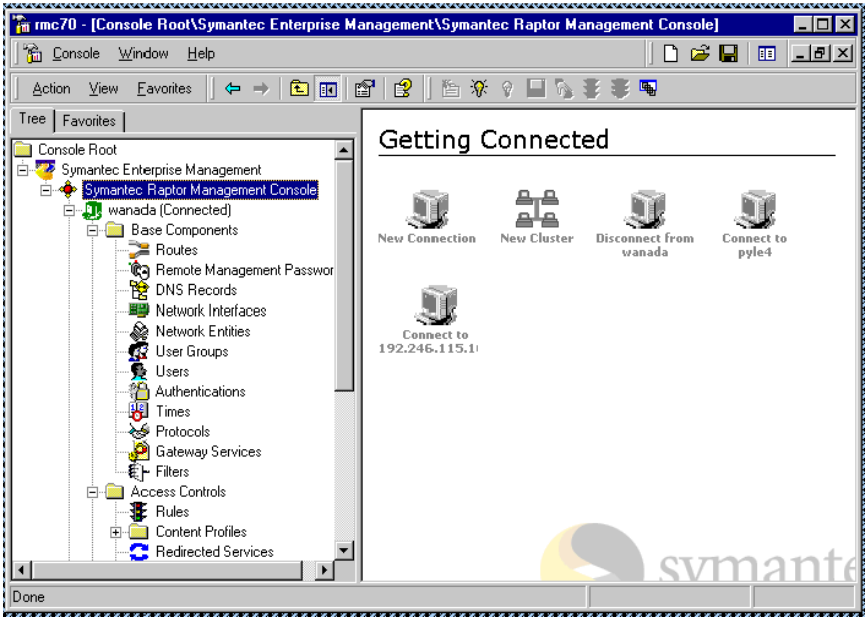


Figure 4-31 Symantec Raptor Management Console

3 To connect to a remote host or to connect to the local host for the first time, click the **New Connection** icon.

or

For local management, click the **Connect to localhost** icon.

The **Symantec Raptor Management Console** Logon dialog box is displayed.

Figure 4-32 Symantec Raptor Management Console Logon

4 For local management, log on to a local machine by entering `localhost` or `127.0.0.1` in the **Name** field and entering your password in the **Password** field.

   For remote management, log on to a remote machine by entering the IP address or the DNS-resolvable name of the remote system in the **Name** field. In the **Password** field, enter the password for the remote system. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for information on creating a password for a remote system using `rempass`.

The management port number defaults to 418. If you are using SRMC for local management, you should not change the port number. You may need to change it to manage an SEF/SEVPN system through another SEF/SEVPN system. For instructions, see the *Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide*.

Uninstalling the SEF/SEVPN products

You can uninstall any of the products on the Symantec Enterprise Firewall Distribution CD by using the appropriate uninstall menu option

1. Select **Uninstall VPN or Firewall Gateway** or **Uninstall Raptor Management Console**, as desired.
2. Confirm that you want to uninstall.
3. Restart the computer when prompted.
4. If you are removing the product permanently from the computer, delete the `\Raptor` or `\Symantec` folder after uninstalling.

Note: If you are uninstalling as a precursor to upgrading, leave the `Raptor` directory on the computer.

You can also uninstall a Symantec Enterprise Firewall or Symantec Enterprise VPN with the following alternate procedure

1. Select **Add/Remove Programs** from the **Control Panel**.
2. Highlight **Symantec Enterprise Firewall**, **Symantec Enterprise VPN**, or **Symantec Raptor Management Console**.
3. Click **Remove** and confirm when prompted.
4. Restart the computer when prompted.

Installing RemoteLog

RemoteLog can be installed on remote systems to allow secure access to remote logfiles. The self-extracting files (`rlog_6-winnt.exe`, `rlog_6-linux.tar`, and `rlog_6-sunosv5.tar`), which are required for RemoteLog, are located on the SEF or SEVPN CD-ROM in the `ClientSoftware\Remotelogs\3DES` or `DES` directory. Use the appropriate file for Windows, Linux, or Solaris clients.

Caution: Do not install the remotelog client on the SEF/SEVPN system. Doing so will overwrite the remotelog server with the remotelog client.

For more information on using RemoteLog, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

How Vulture disables unauthorized services

The Vulture™ program detects and kills services running on the Symantec Enterprise Firewall or Symantec Enterprise VPN gateway that:

- Are not required by the SEF/SEVPN system
- Are not part of the SEF/SEVPN system software
- Are not specified in the `vulture.runtime` file

By default, the Vulture's activation frequency is one minute. You can change this frequency by editing the file `\Raptor\firewall\sg\vulture.runtime`.

Place a new frequency, in seconds, in the file. A value of -1 disables Vulture. You can exempt user accounts and server applications from Vulture on an individual basis. For instance, add a username after the number of seconds parameter in the `vulture.runtime` file. For example:

```
60
Administrator
```

This example sets the Vulture activation frequency to 60 seconds and exempts the user account `Administrator` from being killed.

Chapter 5

Implementing high availability and load balancing

High availability and load balancing with RainWall

This chapter provides instructions for configuring RainWall for use with Symantec Enterprise Firewall (SEF) 7.0 for Windows NT in order to provide a complete secure, highly available, and scalable perimeter solution.

High availability (HA) solutions reduce downtime due to single point of failures in a network. In the event of a gateway failure, a second gateway takes over; any existing connections are lost, but new connections are established immediately. Load balancing (LB) solutions support the distribution of network traffic over two or more security gateways. By distributing traffic over multiple nodes, customers get the benefits of a scalable architecture that can grow as their business grows, in addition to minimizing single point of failures in their network.

Figure 5-1 depicts a typical two-node HA/LB array using SEF and RainWall 1.5. In this example, each firewall has three network interface cards for connecting to the private, service, and public networks respectively. The internal network acts as the heartbeat or control network. The heartbeat network is used by each node in the array to exchange state information about the cluster. For security reasons,

both Symantec and Rainfinity recommend that only physically secured networks be used for node-to-node cluster communication.

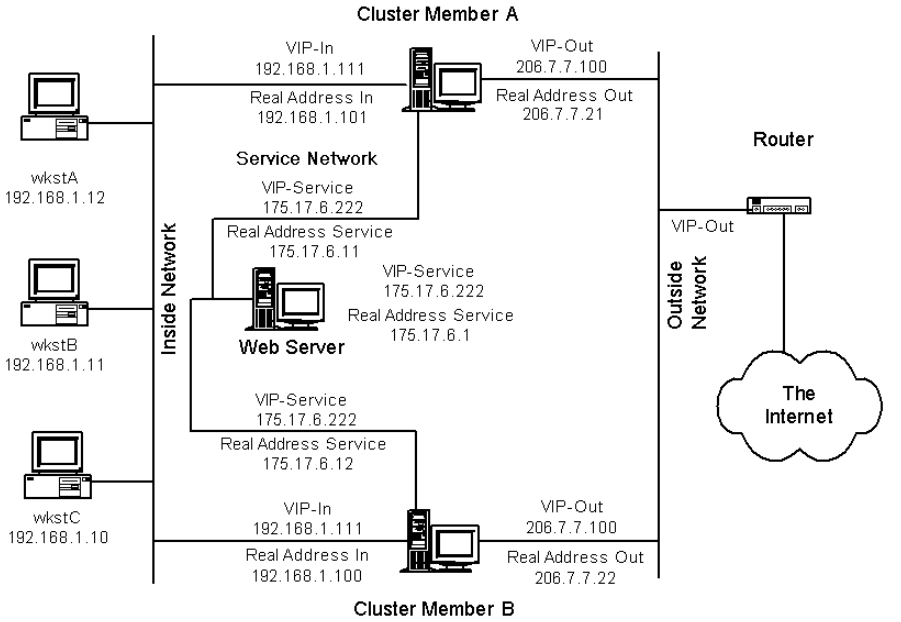


Figure 5-1 Example RainWall configuration

Once RainWall is installed and configured on each firewall on the cluster, the cluster itself is accessible through the assigned Virtual IP (VIP) addresses. On the example network, three VIPs have been assigned: 206.7.7.100 (VIP-Out), 175.17.6.222 (VIP-Service), and 192.168.1.111 (VIP-In).

Note: The VIP address(es) must be higher than the physical IP addresses of the other nodes of the subnet.

Using the configuration in Figure 5-1 as an example, the following network changes would have to be made:

- All internal hosts must point to VIP-In as their default gateway. This ensures that outbound traffic always reaches the “active” gateway.
- All service network servers must point to VIP-Service as their default gateway.
- The external router must point to the VIP-Out address as the next hop to the 206.7.7.0 subnet.

- If you want to hide the Web server's address using service redirects on the Symantec Enterprise Firewall, external DNS resolution requests to www.mywebserver.com will resolve to the VIP-Out address.

The VIP addresses are used as the reference points to all the previous definitions that would otherwise use the real (physical) address of the firewalls. This removes any dependencies on a single firewall, thus eliminating the single point of failure scenario. All communication flows through the VIPs.

The one exception to this rule is for managing the firewalls themselves using the Symantec Raptor Management Console (SRMC). A virtual address cannot be used to manage the firewall because it is impossible to control which firewall is servicing the request. Therefore, all SRMC connections should be directed to the physical IP address of the firewall to be configured, and not the VIP of the array. For example, to manage Firewall A, you would use the real IP address 206.7.7.21.

Based on configuration parameters, only one node in the cluster claims ownership of the VIP. This node, called the incident node, receives all communication requests addressed to the VIP on the array and is responsible for:

- Serving the request
- Passing on the initial request to another node in the cluster (for load balancing)
- Passing on the request to the node that is currently serving the connection

If a failure occurs on the incident node, another node in the cluster claims ownership of the VIP and assumes all responsibility for new connections requests coming to the cluster.

Installation overviews

This section provides high-level overviews of the process for installing and configuring the RainWall 1.5 high availability and load balancing solution, and then installing a Symantec Enterprise Firewall (SEF) 7.0 for Windows NT to operate with RainWall.

Two overviews are provided:

- For new configurations which have not had a firewall installed previously
- For existing firewall configurations to which the RainWall solution will be added

New configurations

Although there are other ways to install and configure these products, by following the suggested process you will minimize risks associated with interoperability issues between the two products.

1 Make sure that your hardware and system configurations are supported by both SEF and RainWall 1.5. For example, SEF currently supports a greater number of NICs types than RainWall 1.5. Therefore, you need to use the minimum common denominator supported by both products for your hardware and operating system versions.

For SEF/SEVPN hardware requirements, see **Hardware and software requirements on page 24**.

For a list of supported network cards for RainWall, see the Rainfinity web site at `http://www.rainfinity.com`.

If you choose to install the RainWall Management Console, you must install the Java 2 Runtime Environment (JRE) version 1.2 or later. This can be obtained from `www.java.sun.com/j2se/1.3/jre/download-windows.html`. The RainWall Management Console is not required to configure RainWall with Symantec Enterprise Firewall. If installed, it should only be used to monitor firewalls.

2 Configure your physical network as though your eventual firewall nodes are routers. In other words, test the connectivity between your internal machines and each of the gateways, and between your service net and your internal network.

Caution: For security reasons, do not connect the gateways to any external network at this time since there is no firewall protecting you yet.

However, do connect the external NICs from each of the cluster nodes to a hub or switch. This is because in order for the nodes to join the cluster, the network connections must be live. If they are not, RainWall thinks that the node is down because of a physical failure and you will not be able to test your array connectivity.

3 Install RainWall on each of the nodes in the array by running `setup` from the `RainWall` directory on the CD.

It is not necessary to install the RainWall Management console. All configuration should be done using the Cluster Wizard, available from the Symantec Raptor Management Console.

4 Install the SEF software on the cluster nodes.

Note: All nodes must have the same licenses to prevent problems with failover.

---

5 Configure the cluster nodes to participate in the RainWall cluster using the instructions on the Cluster Wizard, found in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

This configuration includes the assigning of Virtual IP addresses (VIPs).

Note: The VIP address(es) must be higher than the physical IP addresses of the other nodes in the cluster.

---

6 Change the default routes on your internal and service network hosts to the VIPs of the array. Test connectivity to the VIPs by pinging them from the internal or service network hosts.

7 Test the RainWall functionality by disconnecting one of the network cables from the active or incident node.

If you start to `ping <VIP> -t` continuously before you disconnect the cable, you should see one or two failures at the time you pull the cable; however, almost immediately the other node will start responding to the VIP.

8 Connect the external network to the external router, and make the necessary changes on the external router's routing table to point to the external VIP of the cluster.

Test connectivity and VIP behavior by pinging from the external router.

9 Make necessary changes to your external DNS entries for your service network servers and applications.

10 Configure your security policies, remembering that any references that you would normally make to the SEF interfaces will now be made to the VIPs instead (see **Modifying rules for use with RainWall on page 81**).

You must configure each firewall in the RainWall cluster with identical policies. A mismatched configuration prevents failover from occurring due to differing policies. This can be accomplished by configuring policies on one node and using the Propagate command (documented in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*) to copy the configuration to the other nodes of the cluster.

Existing firewall configurations

Additional steps are required to configure RainWall with an existing Symantec Enterprise Firewall installation.

1 Uninstall the Symantec Enterprise Firewall (SEF). This is required because RainWall must be installed and configured before SEF. Be sure to backup your previous installation, and to disconnect from the network to protect your network security.

2 Install RainWall.

3 Reinstall SEF.

4 Run the New Cluster Wizard to configure the RainWall Cluster and VIPs.

5 Review your existing authorization rules as described in **Modifying rules for use with RainWall on page 81**.

Installing RainWall

This section provides installation recommendations for the RainWall product.

Caution: Do not install RainWall on a machine that already has firewall software running. See **Existing firewall configurations on page 76**.

1 Install RainWall on each node by navigating to the RainWall directory of the SEF/SEVPN CD-ROM and double clicking on the Rainwall executable, Rainwall_1_5_3b92_SEF.exe.

The RainWall Welcome screen appears.

RainWall - InstallShield Wizard
Welcome to the InstallShield Wizard for RainWall
The InstallShield Wizard(TM) will help install RainWall on your computer. To continue, click Next.
< Back
Next >
Cancel

Figure 5-2 RainWall Welcome screen

2 Click **Next** to begin the installation.

Files are extracted and a second welcome screen is displayed.

3 Click **Next**.

You are prompted to agree to a license agreement.

4 Click **Yes** to accept the license agreement.

The Select Components screen appears.

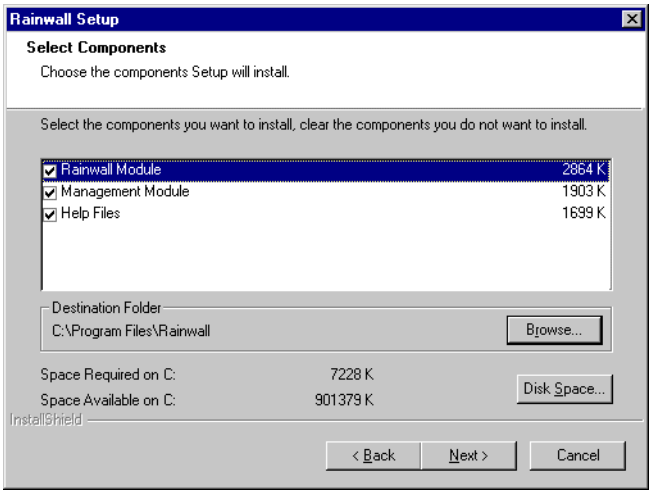


Figure 5-3 RainWall Select Components screen

5 Select the components you want to install.

Symantec recommends that you deselect the Management Module, which installs the RainWall Management Console (RMC). The RMC is not needed because all configuration of the RainWall cluster should be done using the Symantec Raptor Management Console after the Symantec Enterprise Firewall software is installed.

If you do want to install this component, you should install it later inside the protected network on a separate machine that is not running the Symantec Enterprise Firewall.

6 Click **Next**.

After displaying a setup status screen and copying files, the installation prompts you for a RainWall Service Password.

Figure 5-4 RainWall Service Password screen

While this password is required to complete the installation, you will not need it to set up a standard RainWall/Symantec Enterprise Firewall configuration.

It is the local password which is used to manage RainWall using the RainWall Remote Management Console, or when running the rwstat command line interface.

7 Enter and confirm the RainWall password and click **Next**.

After a few moments, the Complete screen appears.

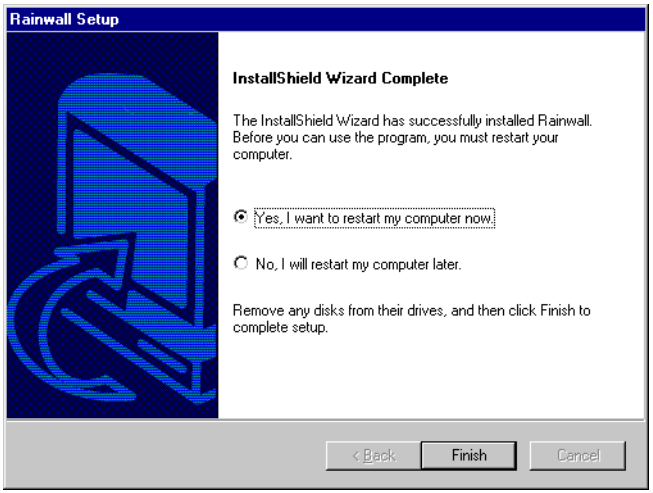

Rainwall Setup
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Rainwall. Before you can use the program, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

Figure 5-5 RainWall Complete screen

8 Click **Finish** to complete the RainWall installation.

Starting and stopping RainWall

To start the RainWall service

1. Select **Start**>**Settings**>**Control Panel**>**Services** to display the **Services** dialog box.
2. Select **RainWall**.
3. Click **Start**.

To stop the RainWall service

1. Quit any instances of the RainWall Remote Management Console that may be running on the local machine.
2. Select **Start**>**Settings**>**Control Panel**>**Services** to display the **Services** dialog box.
3. Select **RainWall**.
4. Click **Stop**.

Installing the Symantec Enterprise Firewall

After you install RainWall, install the Symantec Enterprise Firewall (SEF) as described in one of the sections under **Installation instructions on page 43**.

Note: When you are asked to select inside and outside network interfaces, the choice of NIC cards you are offered reflects the RainWall naming convention: RaincoatMP3, RaincoatMP4, etc., rather than the more familiar E100x or D233x.

Modifying rules for use with RainWall

There are some special requirements when writing rules for SEF and SEVPN systems that are configured with RainWall.

When an existing SEF or SEVPN system is reconfigured to work with RainWall, existing rules should be examined to be sure they do not conflict with the following requirements:

- Interface-based rules

  Because RainWall uses specific names to refer to network interface cards, interface-based rules must use these naming conventions, rather than the industry-standard naming conventions.

- Redirected services

  Rules that involve service redirects must point to the RainWall VIP addresses rather than to real addresses.

Uninstalling RainWall

Note: Before uninstalling RainWall, uninstall the SEF/SEVPN system. For detailed instructions, refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Installation Guide*.

To uninstall the RainWall software

1. Stop the RainWall service and Remote Management Interface.
2. Remove the RainWall program.
3. Remove the RainWall driver.

For detailed uninstallation instructions, refer to the *RainWall User Guide*.

Chapter 6

SEF installation verification

This chapter describes the procedure for verifying that your Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN (SEVPN) installation has been completed correctly.

Troubleshooting possible problems

Though unlikely, it is possible to encounter problems during the installation process.

- Install shell errors
- Missing files
- Use of an incorrect license key

If you encounter any problems during the installation, review **Chapter 3, Pre-installation requirements** and check your system for discrepancies. If error messages continue to appear during the installation, record the information and contact customer support.

For online Symantec Support, visit our "Services and Support" web site: www.symantec.com/techsupp/. Have your SEF/SEVPN software serial number available when you call.

If you have a maintenance contract with an authorized Symantec reseller, contact them for support.

Note: Before calling for support on any problem, refer to the documentation for suggested actions.

If the installation fails

If the installation fails, make sure you are in compliance with each item in **Chapter 3, Pre-installation requirements**. Verify that your hardware is supported. Uninstall, then try to install the SEF/SEVPN product again.

Check basic connectivity

Check your network connectivity. If any of your routing is not set up correctly, it will cause assorted problems.

The easiest way to do this is to use the ping utility. Ping does the following.

- If you enter a host name, ping first does a DNS lookup on that name.
- Once it has an IP address (or if you enter an address), it sends ICMP packets to see if the machine will respond.

A Symantec Enterprise Firewall will not pass ICMP packets unless you have a rule configured which allows it. You cannot ping through the firewall otherwise. For information on configuring rules, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

You can use ping on the firewall machine itself and the VPN server machine to verify connectivity.

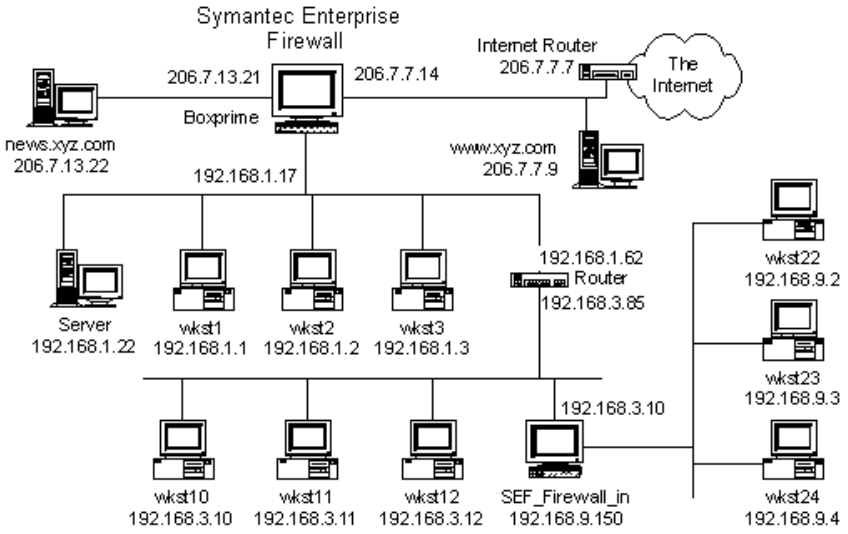


Figure 6-1 Troubleshooting example network

Referring to the network in **Figure 6-1**, on the firewall machine, open a command window and use the `ping` command to do the following:

Ping the security gateway by address

```
ping 206.7.13.21
```

```
ping 192.168.1.17

ping 206.7.7.14
```

All of these pings should return a reply. If they do not:

- TCP/IP is not installed
- TCP/IP is not bound to your network interfaces

Take the following action to correct the problem

1. Uninstall the security gateway, following the instructions included in the installation guide.
2. Install TCP/IP according to your manufacturer's instructions. Use the most current driver.
3. Verify that you can ping these addresses.
4. Reinstall.

From a command prompt window on the firewall machine, ping an address on each of the inside networks

Each ping command should return a reply. For example:

```
ping 206.7.13.22
```

If there is no reply, the specified computer (*news*, in this example) is not on, or does not have TCP/IP installed or bound to its interface. Fix the computer and try again.

```
ping 192.168.1.22
```

Again, if there is no reply, the computer is down or does not have working network connectivity.

```
ping 192.168.3.10
```

If this ping fails, the problem could be the router between the subnets. Ping both addresses (192.168.1.62 and 192.168.3.85). If neither ping yields a reply, your router is off.

If only 192.168.3.85 is not responding, your router is not passing ICMP. Check to see that the router is working. Check its configuration to see if it is filtering ICMP.

```
ping 206.7.7.9
```

This address is on the same subnet as the firewall. If this ping does not return a reply, 206.7.7.9 is not working or does not have network connectivity. (Your network may have a router or bridge between the firewall and this computer. If so, check that piece of equipment.)

```
ping 206.7.7.7
```

If this fails, something is wrong with your connection to the Internet.

- Check your router.
- Check your service provider.
- Try the ping from www.xyz.com (if it works from here, verify that you are pinging a real address and that the address is actually alive).

`Ping` a host on the Internet

```
ping www.symantec.com
```

If this fails:

- Use the trace route command (`tracetr <ip address>`) to find out where the ping failed.
- The routing information on the system may be incorrect. Check its default gateway setting.
- You may be behind another security gateway that does not pass `ping` packets to the Internet.
- The router may not be configured properly.
- The remote system may not be running, connected to the network, or configured properly.
- There may be a packet filter running between your site and the other site. Try another site or try using `ftp` or `telnet` to make the remote connection.

If all of the preceding pings return replies, your basic connectivity is working.

If network connections are unsuccessful

If a machine on the Internet is unreachable, your connection to the Internet or your network card may not be working correctly or it may not be installed properly. Check the following:

- Your outside network card may not be properly installed. It may also not be supported, or it may be defective. Check the Microsoft Hardware Compatibility List (HCL) to make sure your network card is supported.
- Use `ping` to verify general network connectivity.
- Your ISP may be down or your line to the ISP may not be working.

If `ping`ing the internal interface host name fails:

- Your name service may not be working correctly. Try `ping`ing the same interface using the IP address instead of the name.

If you can `ping` a computer by address but not by name:

- You have a name service problem. Check your DNS configuration. Use the manufacturer's troubleshooting information to get your name service working.

If you cannot `ping` an inside system by address, then a connection is not working or there is a problem with routing.

- Your inside network card may not be properly installed. It may also not be supported, or it may be defective. Check the Microsoft Hardware Compatibility List (HCL) to make sure your network card is supported.

If you cannot `ping` a computer behind a router by address, then your static routes are incorrect, your router is not working, or the target host is not configured properly.

- Try `ping`ing both of the router's addresses. If you can `ping` the address closer to you but not the address on the other side, your router is not working or static routes are not established.
- If you can `ping` both addresses, the problem is with the configuration of the computer behind the router.

Installing new network cards

If you install a new physical network interface card, you must uninstall the SEF/SEVPN first, install the card, and then reinstall the product. Your system configuration settings are preserved through the uninstall-reinstall process.

Appendix A

Site pre-installation checklist

Use this checklist to assess your security issues. Knowing your network's requirements as well as its strengths and potential weaknesses will help you optimize the performance of your Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN (SEVPN).

Security planning

1 Does your organization have a security policy?

_____ Yes _____ No

If you checked No, refer to **Chapter 2, Developing a security plan** for information relating to the development of a security policy.

2 Approximate number of users behind your SEF/SEVPN system:

_____

3 Do you plan to establish special groups or users with special privileges that other groups and users will not have?

_____ Yes _____ No

4 Enter the name of the primary administrator:

_____

5 List below all persons involved in administering the system.

Name	Email	Phone	Pager

6 Are organization computer resources accessible by remote dialin?

_____ Yes _____ No

7 What communications servers are used? (Shiva, Annex, Livingston, etc.)

_____

_____

8 What form of authentication will be used for remote access to company resources?

_____ username/password _____ LDAP

_____ CRYPTOCard™ _____ RADIUS

_____ Defender™ _____ S/Key™

_____ Entrust _____ SecurID

_____ TACACs+

9 What mechanism will be used for suspicious activity alerts?

_____ audio notification _____ email

_____ pager _____ Client Program

_____ SNMP V1 _____ SNMP V2

10 Do you plan to manage SEF/SEVPN remotely?

_____ Yes _____ No

11 Do you have a Symantec Enterprise Firewall or Raptor system on your network now?

_____ Yes _____ No

12 If Yes, what brand and version?

_____

Site hardware information

1 Enter the serial number of the SEF/SEVPN host system:

_____

Use the "vol" command to retrieve the serial number of the disk partition on which operating system is installed.

2 Enter type and quantity of network interface cards.

_____ Ethernet Qty: ___ _____ Token Ring Qty: ___

_____ FastEthernet Qty: ___ _____ FDDI Qty: ___

_____ ATM Qty: ___ _____ Other: (type) _____ Qty:___

Before installation, ensure the host network connections are configured and tested properly. Verify that you can ping the network interfaces of the server from clients on the same network. See **Chapter 3, Pre-installation requirements** for further information.

3 Do you have at least 128 MB of memory (256 MB for sites with more than 200 users) on the machine?

_____ Yes _____ No

4 How much memory?_____

5 Enter the number of computers of each type that compose your network:

_____ UNIX computers _____ Windows computers

_____ Other: (type) _____

6 Are you currently connected to the Internet?

_____ Yes _____ No

7 Enter the name of your service provider (ISP):

_____

8 Does your site have, or plan to have, more than one Internet access point?

_____ Yes _____ No

9 Are there any other Internet connections besides the SEF/SEVPN system (such as modems connected to workstations)?

_____ Yes _____ No

10 What network connections do you require for inside and outside networks?

_____ Ethernet _____ Frame Relay

_____ FastEthernet _____ SDN

_____ ATM _____ Token Ring

_____ FDDI

11 Will you be installing the Symantec Enterprise VPN Client or an earlier version of the RaptorMobile product from Symantec?

_____ Yes _____ No

TCP/IP address

1 Do you currently run Domain Name Services (DNS) on your network?

_____ Yes _____ No

2 What type of domains are at your site?

_____ Single domain _____ Multiple domains

_____ Subdomains

3 What type of name service do you provide?

_____ Primary name services _____ Secondary name services

4 List the domain names supported by this site:

_____

5 Do you have an internal name server selected?

_____ Yes _____ No

6 Do you have someone at your site who is knowledgeable about, and comfortable working with, DNS and how to configure it properly?

_____ Yes _____ No

7 Check the address types being used at your site:

_____ Registered IP address _____ Private IP address (RFC 1918)

_____ Unregistered IP address Made up IP address?

Your connection to the Internet must have at least one public network address. Symantec is not responsible for acquiring or registering public IP addresses. The internal (behind the SEF/SEVPN system) addresses do not have to be legal or registered. We strongly recommend that you use private, RFC 1918-compliant addresses internally.

8 List the address ranges currently being used in your network:

9 List the protocols being used in your network:

Note: Only the IP protocol can be directly handled by the SEF/SEVPN system. Other protocols such as IPX cannot be serviced or passed through the SEF or SEVPN system.

E-mail information for firewall notifications

1 Check the type of mail server being used:

_____ In-house mail server _____ Third-party provided

2 Enter the name and IP address of your mail server:

Name:_____

Address:_____

3 Check the transport protocol being used for email:

_____ SMTP mail _____ POP mail

4 Does your Internet Service Provider provide a Mail Relay host? If so, list its name and IP address.

_____ Yes _____ No

_____ Mail Relay host: _____

_____ Address: _____

5 List any mail programs you use internal to your network (ex: CCmail):

_____

News service

1 Will you be using network NEWs services (NNTP protocol)?

_____ Yes _____ No

2If yes, and you have your own internal NEWs (NNTP) server, enter its IP address and the address of the server that will be supplying you with NEWs feeds.

_____ Internal server: _____

_____ External NEWs server: _____ _

Special services

Enter the names of any special services you wish to pass through the SEF/SEVPN system:

Service name Service port # Service type (UDP/TCP) Server name

_____

_____

_____

_____

Allowed TCP/IP Service

1 Check the type of access (if any) you will allow for the following services:

TELNET __ All users __ All internal users __ Selected group __ No access

FTP put __ All users __ All internal users __ Selected group __ No access

FTP get __ All users __ All internal users __ Selected group __ No access

Gopher __ All users __ All internal users __ Selected group __ No access

HTTP __ All users __ All internal users __ Selected group __ No access

2 List your TCP/IP services:

	Group	Authentication	Access times
FTP put			
FTP get			
TELNET			

HTTP

Other

Over time, you will likely refine these permissions. You should make periodic updates to this list.

3 Do you need transparent access from outside the SEF/SEVPN system?

_____ Yes _____ No

Web service information

1 Will you be using a web server?

_____ Yes _____ No

2 If yes, check the location of the web server:

_____ Internal to the SEF/SEVPN system

_____ External to the SEF/SEVPN system

3 Enter the Web server name and IP address:

Name: _____ Address: _____

4 Will you be using an External Caching/Proxy Server? If yes, enter the server name and IP address.

_____ Yes _____ No

Proxy server name:_____ Address:_____

5 Do you plan to use the WebNOT service for Symantec Enterprise Firewall?

_____ Yes _____ No

6 Do you plan to restrict access to any specific URLs?

_____ Yes _____ No

7 If yes, list the URLs to be restricted:

_____

_____

_____

Access lists

In the following sections, list those entities and users you plan to write rules for, allowing them access through the SEF/SEVPN system.

Entities allowed through the SEF/SEVPN system

IP address/DNS name	Entity type	Internal/external

Users allowed through the SEF/SEVPN system

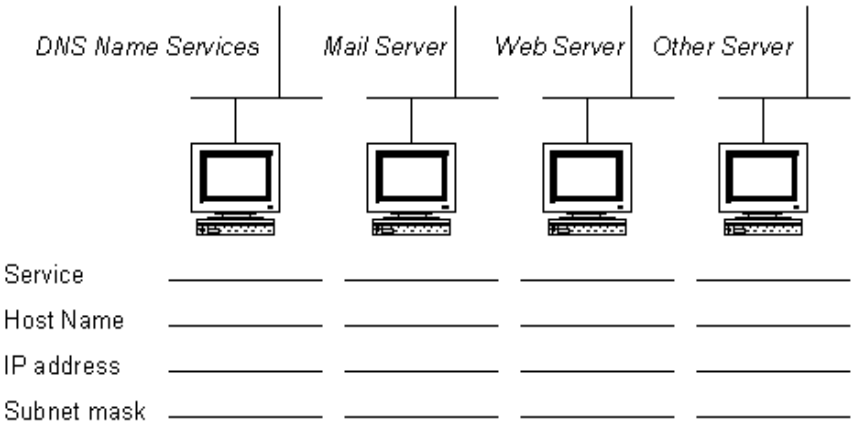
User name	Account name	Group name

Continue on a separate sheet, if necessary.

Network architecture with a SEF/SEVPN system

In the following sections, list all of the entities that comprise your network. Please be sure to show all routers and computers systems that will be directly affected by, or connected to, the SEF/SEVPN system and its directly connected networks. Please label each network component with its IP address and network mask.

1 Your internal network can have a number of servers. List them.

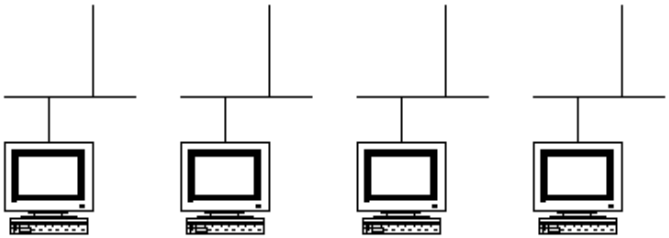


2 Your external network consists of at least the SEF/SEVPN host and a router. Enter your SEF/SEVPN host system and router IP addresses.

IP address	Internal or external?

Router	IP address

3 Your external network can also include external servers, such as an external web server. List all servers here.



Service				
Host Name				
IP address				
Subnet mask				

Index

A

Access lists
    checklists 99
Access method
    general 19
    VPN 20
Authentication method
    checklist 91
Authorization rules
    with application proxies 19
    with GSP 20

C

CIFS/SMB
    proxies 19
Configuration utility
    for SEF or SEVPN 65
Connecting
    to Symantec Enterprise Firewall 67
    to Symantec Enterprise VPN 67

D

DHCP
    restriction with SEF/SEVPN 25
Disabling
    unauthorized services using Vulture 70
DNS
    testing entries 34
DNSd
    configuring for Windows 2000 28, 30
Domestic encryption
    choosing 43, 53, 57
    compatibility issues 23
Drive format
    for installation of SEF/SEVPN 25
Dynamic Host Configuration Protocol
    see DHCP

E

E-mail information
    checklist 94
Encryption type
    choosing 43, 53, 57
    compatibility issues 23
Entities
    mapping for network security planning 15
External servers
    identifying for site security plan 17

F

FTP
    proxies 19, 35

G

General access options 19
Generic Service Passer
    See GSP
Gopher
    proxies 19, 35
Groups
    defining for site security plan 18
GSP
    authorization rules

H

Hardware requirements
    for Symantec Enterprise Firewall 24
    for Symantec Enterprise VPN 24
Heartbeat network
    description 71
High availability

description 71
installation overview 74
Host system interfaces
testing 33
HTTP
proxies 19, 35

I

Incident node
for RainWall 73
Installing
remotelog 69
Symantec Enterprise Firewall 43, 57
Symantec Enterprise VPN 43, 57
Symantec Raptor Management Console 53
Windows NT and Windows 2000 37, 43
Internal servers
identifying for site security plan 17
International encryption
choosing 43, 53, 57
compatibility issues 23
Internet service
prerequisites 35
IP addresses
checklist 93
procuring 35
setting for Windows 2000 27
verifying 31

L

License key
changing after installation 66
entering 45, 60
obtaining 42
Load balancing
description 71
installation overview 74
Local Firewall Management 68
localhost
connecting to 67

M

Microsoft Internet Explorer
required for SEF/SEVPN 26
Modem
prerequisites 26

N

Name resolution
planning 34
Network architecture
checklist 101
network planning worksheet 16
Network configuration
testing 31
Network connectivity
checking after installation 85
checklist 93
testing example 32
troubleshooting 88
Network information
collecting for site security plan 18
Network Interface Cards
see NICs
Network interface configuration
changing 65
Network settings
testing 31
Windows 2000 27
Windows NT 29
News service
checklist 95
NICs
assigning subnets 25
assigning TCP/IP protocol
on Windows 2000 27
on Windows NT 29
checklist 92
configuring after installation 65
installing new 88
requirements 25
specifying interfaces 51, 63
NNTP
proxies 19, 35

O

Operating system
configuring 25
supported platforms 24

P

PowerVPN
uninstalling 39
upgrading 38
upgrading after file system change 40
Pre-installation
checklist 89
tips 34
Proxies
authorization 35
authorization rules 19
checklist 96

R

RainWall
example configuration 72
installing 77
installing Symantec Enterprise Firewall 80
starting 80
stopping 80
uninstalling 81
RainWall cluster
example 72
Raptor Firewall
uninstalling 39
upgrading 38
upgrading on Windows 2000
after file system change 40
RealAudio
proxies 19, 35
Registering
Symantec Enterprise VPN 36
Remote Firewall Management 68
Remote host
connecting to 67
remotelog
installing 69
Routing tables
requirements 26

S

secure HTTP
proxies 19, 35
Security plan
checklist 90
defining 12
developing 12
network planning 16
site configuration example 13
worksheets 15
Service network servers
identifying for site security plan 17
Site hardware information
checklist 92
Site security plan
collecting network information 18
defining users and groups 18
developing 12
external servers 17
internal and external entities 15
internal servers 17
service network servers 17
site configuration example 13
SMTP
proxies 19
Software requirements
for Symantec Enterprise Firewall 24
for Symantec Enterprise VPN 24
Sound card
prerequisites 25
SQL*Net
proxies 35
SRMC
installing 53
logon 68
opening 67
uninstalling 69
subnets
assigning for NICs 25
Symantec Enterprise Firewall

configuration utility 65
connecting to 67
cross platform management 23
hardware requirements 24
installing 43, 57
on RainWall 80
supported features 23
uninstalling 69
verifying installation 83
Symantec Enterprise VPN
configuration utility 65
connecting to 67
cross platform management 23
hardware requirements 24
installing 43, 57
obtaining license key 36
registering 36
supported features 23
uninstalling 69
verifying installation 83
Symantec Raptor Management Console
see SRMC

T

TCP/IP
checklist 93
protocol
on Windows 2000 27
on Windows NT 29
services
checklist 96
setting host name
Windows NT 29
setting options for Windows 2000 28
setting options for Windows NT 30
verifying connectivity 31
verifying settings 31
Telnet
proxies 19, 35
Testing
basic connectivity 85
network configuration 31
Tips
pre-installation 34
Troubleshooting
example network 85
failed installation 84
possible problems 84

U

Unauthorized services
killing with Vulture 70
Uninstalling
PowerVPN 39
RainWall 81
Raptor Firewall 39
Symantec Enterprise Firewall 69
Symantec Enterprise VPN 69
Symantec Raptor Management Console 69
Upgrade procedures 38
Users
defining for site security plan 18

V

VIP addresses
for RainWall
Virtual IP addresses
see VIP addresses
Virtual Private Network
See VPN
VPN
access options
Vulture
disabling unauthorized services 70
setting activation frequency 70

W

WEB service
checklist 98
Windows 2000
configuring for DNSd 28, 30
network settings 27
pre-installation settings 25
setting computer name 27
setting IP addresses 27

setting TCP/IP options 28
Windows NT
network settings 29
pre-installation settings 25
setting computer name 29
setting TCP/IP host name 29
setting TCP/IP options 30
Windows NT and Windows 2000 installation 37
Worksheets
security planning 15, 89